Design of Student Attendance System Using Internet of Things (IoT) Technology

Banu Santoso¹, Marti Widya Sari²

¹Computer Engineering Department, AMIKOM University, Yogyakarta, Indonesia
²Informatics Department, Universitas PGRI Yogyakarta, Yogyakarta, Indonesia

¹banu@amikom.upy.ac.id, ²widya@upy.ac.id

Abstract. Lecture attendance data at universities is a reference in showing the credibility of each student used by lecturers as data for student grades as well as an evaluation material for the success of teaching and learning activities in lectures, but there are several examples of cases related to student attendance data currently prevalent in the world of education or lectures is the phenomenon of "Leave Absence" or better known as TA. In addition, other problems also arise from lecturers and administrative staff, namely difficulties in monitoring student attendance and efforts to validate attendance data because of the large amount of student data. Therefore in this study a system was proposed to reduce the level of fraud in filling the attendance list and effectiveness of student data processing using a system of applying the concept of the Internet of Things (IoT) with the fingerprint presence method. Existing system modeling results are expected to be able to support the service of processing academic data automatically and produce accurate and accurate statistical data and be able to reduce data manipulation factors from irresponsible parties.

1. Introduction

Along with the development of the present time people are required to proceed faster in all things because technology is developing so rapidly with various emerging innovations and their application, which greatly helps people's daily activities and the application of advanced technology is felt in all aspects, one of them in academic lectures aimed at facilitating the process of academic service, one of the uses of information technology is the lecture attendance system at universities. The existing attendance data is used as a reference to show the credibility of each student [1] besides that it is used by lecturers as data for student grades and also as an evaluation material for the success of teaching and learning activities in lectures. Attendance is very important for students who are required to attend lectures at least 75%, which determines whether the student is eligible to take the semester exam or not, besides that most lecturers make it as a component of assessment [2].
Although some universities still use class attendance systems that still use conventional signatures and also use barcodes found on Student Identity Cards (KTM) as attendance data inputs, the two methods are considered to be less effective in supporting student learning activities. These problems not only arose from the students but also the campus academics who also had difficulties in administration and management of campus data. Therefore we need a solution that uses a new innovation related to the presence of lectures to reduce the level of fraud in filling the attendance list and the effectiveness of processing student data using the fingerprint presence system. The fingerprint presence system is a fingerprint presence mechanism as a symbol of identity using a computerized tool [3].

The implementation of this fingerprint-based presence system uses the concept of Internet of Things (IoT) which is a form of network that has the ability to connect various objects that have identities and IP addresses, so that they can communicate and exchange information about themselves or the environment they reach [4]. In addition, the fingerprint authentication model has been widely used widely because the model makes it easier for users to do attendance and also avoids the presence of data manipulation [5]. So that the fingerprint attendance system aims to prevent students who falsify their presence in addition to saving more time in taking attendance, therefore based on the above problems, the researcher makes a presence design that is considered more effective and efficient that can reduce errors in the identification process through the application of Internet concepts of Things (IoT) with the fingerprint method.

2. Literature Review

For research conducted by Dhanalakshmi, et al. [6], it presents research using Fingerprint and GSM / GPRS modules. The biometric attendance system is designed and implemented to monitor efficient real-time and transparency in managing the actual presence of students using wireless fingerprint terminals based on GSM - Wireless Fingerprint Terminals (WFTs). This system is suitable if applied in educational institutions. Each individual has a unique fingerprint pattern that motivates its use to conduct biometric authentication and is verified to find student attendance at the institute. There are two approaches to authenticating fingerprints taken in the verification process, namely, the first approach uses a database created by the organization itself and the second approach uses Aadhaar Central Identification Repository (CIDR). Using the original presence of WFT from students can be recorded, monitored and maintained without any interference from humans. Attendance reports can be automatically sent directly to students and their parents' cell phone numbers via SMS so as to provide transparency in addition to promoting efficient attendance system management and improving academic quality.

This research was conducted by Vantová, et al. [7], presenting an application for managing attendance systems by making attendance lists. This administrative application is made to avoid manipulation through the attendance system, in addition to providing a safe and reliable way to evaluate student attendance in certain lectures and complete assignments. This application uses NFC technology on smartphones and RFID cards as student cards, whose ownership is required for every student at the
university. NFC technology has the ability to record student identity on student cards. This research was conducted by Chaniago, et al. [8], presenting a student attendance application based on the SMS Gateway application that was made to ensure that students attend classes, with the following steps: students must submit an identity card to the teacher in charge, then the teacher scans the barcode printed on the card, and finally the data will be stored in the database automatically. This application provides services for parents to find information on a weekly and monthly basis. This application can also be taken into consideration in making decisions for principals by downloading student attendance data in the Microsoft Excel file format. The implementation of SMS gateway-based applications for student attendance in schools is expected to be the solution to students' absenteeism problems due to skipping school. With the construction of this system, parents can monitor their children by obtaining information in the form of text messages sent from school management to the presence of children at school.

This research was conducted by Lodha, et al. [9], presenting attendance applications using Bluetooth and RFID. This technology uses electronic tags to identify wireless automatically, with Bluetooth enabled devices. Bluetooth-based student attendance applications can shorten time and reduce human error factors that are often at manual presence. This application also generates student attendance statistics, making it easier for school management to make further decisions. The main advantages of this system include low power consumption, high data transfer, small chip size and low cost and easy implementation of these devices.

This research was conducted by Noor, et al. [10], by changing the conventional method which is still adopted in several educational institutions, such as lecturers calling on student names one by one or by taking signatures from each student to determine attendance attendance. Currently, a better method has also been used, namely by relying on a system to record student attendance semi-automatically. For example RFID or biometric based systems. Such a system has become the solution to existing problems, but the disadvantage is the additional cost of hardware maintenance. This application, once installed, can be used to download a list of students from a web server. Based on the list of students downloaded, the device will then act like a scanner to scan each student card one by one and confirm and verify the student's whereabouts. While the camera device is used as a sensor that reads barcodes on student cards. Updated attendance lists are then uploaded to the online database and can also be saved as files to be transferred to the PC. While in this study using attendance system design modeling of student attendance at the university by utilizing fingerprint and Internet of Things (IoT), so that modeling the system can reduce fraud or manipulation in the presence system. In addition, attendance data processing is useful for the student assessment system and monitoring student attendance at each theoretical and practical class lecture meeting.

3. Theory

3.1 IoT (Internet of Things)

Internet of Things (IoT) is a design of special hardware, system software, Web API, protocol to be able to connect to the internet [11] [12]. Devices can connect to the internet using Ethernet, WIFI, Bluetooth, Zigbee and so on [13] [14] however, these devices cannot be connected directly to the internet, and are grouped in clusters, for example sensor networks can be connected to the base station (connected to
internet) [15]. Through the application of the Internet of Things (IoT) a network can connect many objects that have an identity with an IP address that aims to expand the benefits of internet connectivity in sharing information and communicating between themselves and the environment that is reached, this can change perceptions about the understanding of the internet depends on limited computer device connectivity. The workings of IoT are by utilizing programming arguments with each command from an argument resulting in interaction and communication between fellow machines that are automatically connected and the connecting media between these devices is the internet.

3.2 Arduino Fingerprint

The fingerprint machine [17] is one of the Biometric Indicators that identifies the existence of each person because everyone has a fingerprint that is different from one another. Through the use of fingerprints it is possible to avoid fraud in presence. The application of the fingerprint method has now developed with the help of sophisticated technology tools with the help of special software that is widely applied in various agencies for the implementation of administrative and service activities.

The use of fingerprint is also very simple because it can directly record itself or prove its presence by attaching one finger on the screen / monitor that is available on the presence machine. Presence data collection using fingerprint is very more accurate, each person has different fingerprints so there is no more entrusted presence attendance. The way the fingerprint machine works is to scan the finger by attaching it to the tool. The recording or recording results will be absorbed by the server section. [18]

3.3 Arduino Uno R3

The word Arduino comes from Italian, Arduino is difficult while no is no. Arduino is also a platform for making open source electronic prototypes for both easy-to-use hardware and software. It has 14 input pins from digital output where the 6 pins can be used as PWM outputs and 6 analog-analog input input pins, 16MHZ crystal oscillator, USB connection, power jack, ICSP head, and reset button. This Arduino uses a microcontroller chip with the Atmel AVR ATMega328 type so that the Arduino can be programmed using a computer as needed. The advantages of Arduino have USB communication facilities and are equipped with a complete library, as well as ready-made modules that can also be used on the Arduino board. For example shield GPS, Ethernet, SD Card and others [19].

3.4 Ethernet Shield

Ethernet shield is a device that provides capabilities for the Arduino microcontroller to become a web server or network that is connected to a computer or internet network. The working system of this device is done by installing an Arduino module on the board, then connecting to the network via an RJ45 cable and then following the instructions. Ethernet shield has similarities with NIC (Network Interface Card) which functions to receive or send data on a computer network. The Ethernet shield is equipped with an Ethernet Wiznet W5100 chip and an Ethernet library used in writing data programs [20].
3.5 ESP8266 MCU Code

ESP8266 [21] is an enhancement to a microcontroller such as Arduino so that it can connect directly with WIFI and establish a TCP / IP connection. ESP8266 has deep sleep mode, so that the use of power will be relatively much more efficient than the WIFI module. This module requires around 3.3v power with three WIFI models namely Station, Access Point and a combination of both. This module serves to connect a system with an internet network through a wireless signal [22].

3.6 Cloud Thing Speak

Thing Speak is an open source application of the Internet of Things (IoT) and API for retrieving, storing, analyzing, visualizing and actualizing data from sensor or actuator readings on internet-based cloud applications or through Local Area Networks using the HTTP protocol. Thing Speak is also able to create sensor recording applications, location tracking applications, and social networks with Thing Speak status updates [24].

4. Method

To design a data system presence really needs two interconnected devices, namely hardware and software.

4.1 Research Material

The material and material in this study apply the Internet of Things and Fingerprint (IoT) model to the presence of student lectures which is very useful for the campus to be able to ensure and control student attendance at the university.

4.2 Research Tools

This smart presence application requires some hardware and software. The hardware is available in the registration room, several classrooms and server rooms. The main devices / components used for student attendance data systems include the following: Arduino Uno R3, Ethernet Shield, LCD module (Liquid Cristal Display), LAN network cable, Fingerprint, NodeMCU with ESP 8266 modules and Computers. While software in the form of Arduino IDE, Cloud Thingspeak, MySQL Database and Node.JS.

4.3. Arduino Uno R3 and Ethernet Shield

The Arduino Uno R3 board is a microcontroller based on the Atmega328 chip and placed in the registration room for student data input and fingerprint validation. While the Ethernet Shield connects the register node to the smart presence application in the server room.
4.4. Fingerprint

Fingerprint is hardware that is designed to meet fast data needs by using fingerprint verification placed in the registration room, and several classrooms. Student data stored in the fingerprint is used as student attendance data.

4.5. NodeMCU based on ESP 8266

NodeMCU is an electronic board based on the ESP-8266 chip with the ability to perform the functions of a microcontroller and also an internet connection (WI-FI). This NodeMCU has several I / O pins so that it can be developed into a monitoring and controlling application on an IoT project that connects Wi-Fi on a TCP / IP connection using the ESP8266 Wi-Fi module. This study uses the NodeMCU Module which will be placed in several classrooms connected to the Fingerprint module device. While the ESP8266 module consists of a processor, memory and GPIO which is adjusted to the type ESP8266, besides that firmware also uses the AT Command device and also the SDK firmware, where the device used is based on open source, among others, as follows.

a. CodeMCU.

Using C language programming.

b. Micro Python

Using Python programming.

c. AT Command.

Using AT Command commands from the above programming can be used using ESPlorer as Firmware which is based on MCU Node. Besides that it can also use Putty to be used as a control terminal in the AT Command Arduino Uno, and can also be used as a program by adding the ESP8266 library.

4.6. LCD

The LCD module (Liquid Cristal Display) displays information and attendance for student attendance. This LCD module is placed in the registration room and several classrooms.

5. Design and Analysis

5.1 Analysis of System Problems and Needs

Attendance and professionalism of each student. The application of conventional presence is still said to be very efficient and efficient in attendance by way of preservation. This problem solving effort is done by creating a new presence model by making Internet of Things and Fingerprint Modeling. This modeling work system began with a fingerprint through the Fingerprint module, after which the student's self data would appear on the Node Register, then recorded data would be sent to the Server. Whereas
during lecture attendance, the Fingerprint module is connected to the Class Node will send the student attendance data to the Server through the ESP8266-based NodeMCU using a WIFI or internet connection. So that student attendance data can be read in the smart application via the ThingSpeak cloud on the browser server.

5.2 Design of System

The design of the smart presence system in Figure 1 has several stages of the work process, while the stages of the process are carried out as follows. The first stage is that students will register by filling out the form, after which the operator will enter the form data to the computer along with recording the fingerprint of the student through the Fingerprint module on the Register Node. The operator will send the data to the server to save to the database. The second stage is when students enter during lectures in class, the activities that are carried out for the first time are attendance by using fingerprints in the Class Node supervised by lecturers who teach the subject. Then all student attendance data will be sent from the Class Node through the ThingSpeak cloud and then the presence attendance data will be stored on the Server. For the third stage, namely when students enter during lectures in the next class or other, the attendance will be done first through the Class Node and supervised by lecturers, then student attendance data will be sent from the Class Node through Cloud ThingSpeak to Server.

![Figure 1. The design of the smart presence system](image-url)
5.3 Flowchart System

The flowchart in Figure 2 is a Smart Presence work system, the first Lecturer will login after it is followed by the selection of available courses such as courses X, Y and Z. When class status is opened, students are allowed to attend, if when the presence is not successful or has not been detected through the Fingerprint module, the student can repeat the presence again. When successful, students will be present at the lecture, then the data will be sent via the NodeMCU ESP8266 module to Cloud ThingSpeak. After that, the lecture system is closed.

The process of running this research begins with modeling the Internet of Things and Fingerprint which is used for the implementation of fingerprint sensitization. The work system of this modeling begins with scanning the finger of the student, then fingerprint automatically detects the student's fingerprint when doing the presence, then the results of the scanning process are automatically stored in the application that was created using NodeJS and MySQL.
6. Conclusion

Presence system modeling based on the Internet of Things with Fingerprint is expected to be able to support the service of processing academic data automatically and generate statistical data based on the presence of students in each theory and practicum class lecture. In addition, this presence system reduces data manipulation factors from irresponsible parties, so that the data can be monitored indirectly by lecturers.
References

[1] A. Fadlil, K. Firdausy, and F. Hermawan, “Pengembangan Sistem Basis Data Presensi Perkuliahan Dengan Kartu Mahasiswa Ber-Barcode,” J. Telkomnika, vol. 6, no. 1, pp. 65–72, 2008.

[2] Y. Rafita, “ANALISIS FAKTOR-FAKTOR YANG MEMPENGARUHI KECURANGAN AKADEMIK (TTITP ABSEN) PADA MAHASISWA S1 FAULKUTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM UNIVERSITAS ISLAM INDONESIA,” Khazanah J. Mhs., vol. 5, no. 2, pp. 25–37, Jan. 2013.

[3] R. Verawati, “PENGENALAN SIDIK JARI BERDASARKAN STRUKTUR MINUTIAE DENGAN METODE BACK PROPAGATION,” Pelita Inform. Budi Darma, vol. 7, 2014.

[4] E. D. Meutia, J. Teknik, E. Universitas, and S. Kuala, “Internet of Things–Keamanan dan Privasi,” in Seminar Nasional dan Expo Teknik Elektro ISSN, 2015, pp. 2088–9984.

[5] A. Fakih, I. K. Raharjana, and B. Zaman, “Pemanfaatan Teknologi Fingerprint Authentication untuk Otomatisasi Presensi Perkuliahan,” J. Inf. Syst. Eng. Bus. Intell., vol. 1, no. 2, pp. 41–48, 2015.

[6] N. Dhanalakshmi, S. G. Kumar, and Y. P. Sai, “Aadhaar Based Biometric Attendance System Using Wireless Fingerprint Terminals,” in 2017 IEEE 7th International Advance Computing Conference (IACC), 2017, pp. 651–655.

[7] Z. Vantová, J. Paralič, and V. Gašpar, “Mobile application for creating presence lists,” in 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), 2017, pp. 000223–000228.

[8] M. B. Chaniago and A. Junaidi, “SMS Gateway and barcode technology for presence of students in SMK Unggulan Terpadu PGII Bandung: A case study,” in 2016 4th International Conference on Cyber and IT Service Management, 2016, pp. 1–4.

[9] R. Lodha, S. Gupta, H. Jain, and H. Narula, “Bluetooth Smart Based Attendance Management System,” Procedia Comput. Sci., vol. 45, pp. 524–527, Jan. 2015.

[10] S. A. M. Noor, N. Zaini, M. F. A. Latip, and N. Hamzah, “Android-based attendance management system,” in 2015 IEEE Conference on Systems, Process and Control (ICSPC), 2015, pp. 118–122.

[11] A. Junaidi, “INTERNET OF THINGS, SEJARAH, TEKNOLOGI DAN PENERAPANNYA : REVIEW,” J. Ilm. Teknol. Inf. Terap., vol. 1, no. 3, Aug. 2015.

[12] M. W. Sari, P. W. Ciptadi, and R. H. Hardyanto, “Study of Smart Campus Development Using Internet of Things Technology,” IOP Conf. Ser. Mater. Sci. Eng., vol. 190, no. 1, p. 012032, 2017.

[13] B. Santoso, A. Bejo, and A. E. Permanasari, “PERBAIKAN WAKTU TUNGGU PELAYANAN PASIEN RUMAH SAKIT MENGGUNAKAN TEKNOLOGI RFID DAN WSN,” Semin. Nas. Teknol. Inf. Dan Komun. Univ. Atma Jaya Yogyak., p. 8, 2016.

[14] B. Santoso, I. W. Mustika, and S. S. Kusumawardani, “PEMODELAN MONITORING PEMAKAIAN DAN PENGHEMATAN ENERGI LISTRIK DENGAN TEKNOLOGI JARINGAN SENSOR NIKABEL,” Semin. Nas. Teknol. Inf. Dan Komun. Univ. Atma Jaya Yogyak., p. 8, 2014.

[15] B. Santoso, “IMPLEMENTASI WIRELESS SENSOR AND ACTUATOR NETWORK BERBASIS PROTOCOL ZIGBEE UNTUK PEMANTAUAN DAN PENGENDALIAN SMART HOME,” J. Din. Inform., vol. 7, no. 1, pp. 13–31, Feb. 2018.

[16] S. Li, L. D. Xu, and S. Zhao, “5G Internet of Things: A survey,” J. Ind. Inf. Integr., vol. 10, pp. 1–9, Jun. 2018.
[17] R. Cahyaningtiyas, R. Arianto, and E. Yosrita, “Fingerprint for automatic Door integrated with Absence and User Access,” in *2016 International Symposium on Electronics and Smart Devices (ISESD)*, 2016, pp. 26–29.

[18] M. A. Kader, M. Y. Haider, M. R. Karim, M. S. Islam, and M. M. Uddin, “Design and implementation of a digital calling bell with door lock security system using fingerprint,” 2016, pp. 1–5.

[19] N. S. Kumar, B. Vuayalakshmi, R. J. Prarthana, and A. Shankar, “IOT based smart garbage alert system using Arduino UNO,” 2016, pp. 1028–1034.

[20] M. Kusriyanto and B. D. Putra, “Smart home using local area network (LAN) based arduino mega 2560,” 2016, pp. 127–131.

[21] S. Barai, D. Biswas, and B. Sau, “Estimate distance measurement using NodeMCU ESP8266 based on RSSI technique,” in *2017 IEEE Conference on Antenna Measurements Applications (CAMA)*, 2017, pp. 170–173.

[22] R. K. Kodali and A. Naikoti, “ECDH based security model for IoT using ESP8266,” 2016, pp. 629–633.

[23] A. I. Abdul-Rahman and C. A. Graves, “Internet of Things Application Using Tethered MSP430 to Thingspeak Cloud,” in *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2016, pp. 352–357.

[24] S. Pasha, “Thingspeak Based Sensing and Monitoring System for IoT with Matlab Analysis,” vol. 2, no. 6, p. 5, 2016.