Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021)
IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2

ONGULANKO: An IoT Based Biometric Attendance Logger

Fahim Faisal
Dept. of CSE
Daffodil International University
Dhaka, Bangladesh.
embeddedfahim@gmail.com

Syed Akhter Hossain
Dept. of CSE
University of Liberal Arts Bangladesh
Dhaka, Bangladesh.
akhter.hossain@ulab.edu.bd

Abdus Sattar
Dept. of CSE
Daffodil International University
Dhaka, Bangladesh.
abdus.cse@diu.edu.bd

***Abstract*—Internet of Things (IoT) is shaping our lives by changing the way the information are collected and processed. On the other hand, biometrics is rapidly gaining popularity in the field of automatic person identification. Combining these two technologies, this research work aims to create a smart attendance management system which automates the process of attendance recording in institutions of higher learning, thus, saving both effort and valuable time of educators. This paper discusses about ONGULANKO, which is a prototype of such a system. Attendance of a particular student is automatically uploaded to a remote webserver as soon as he/she places his/her fingertip on top of the device. Attendance, class/course and student records are all stored in the remote server's database. From the website of the system, these records can be viewed, modified, deleted and downloaded as a CSV file as per the user's need.**

***Keywords*—IoT, Biometrics, Fingerprint, Feature Extraction, Enrollment, Matching, Fingerprint Sensor, Microcontroller**

I. INTRODUCTION

With the decrease in cost and increase in availability of portable computing devices, various physical and environmental sensors and the internet, there has been a lot of research and advancement in the field of Internet of Things (IoT). IoT tries to find solutions to real-world problems by adding sensing, processing and networking capabilities to things or objects which normally don't have these capabilities. This makes them capable of collecting and passing data to other IoT devices through a local network or the internet. The devices form a giant web which can collect data on an unprecedented scale and the data helps to efficiently solve real-world problems.

Biometrics is anything and everything that can be measured in human beings. It is used to determine physiological and behavioral characteristics of individuals. These characteristics include: fingerprints, voice patterns, facial images, retinal images etc. Using biometrics, a person can be accurately identified given the precise acquisition of biometric data. In our case, fingerprints are used as biometric data. The word "ONGULANKO" means fingerprint in Bangla. Fingerprint is a unique feature of an individual, i.e., fingerprints of two different people are very rarely the same.

"Two like fingerprints would be found only once every 1048 years" — Scientific American, 1911.

This plays a very important role in identification processes and it is required to utilize fingerprint verification as a means of detecting presence of a particular student in a particular class. As technology moves forward, more information is available to the students through the internet, which in turn, decreases their interest in attending classes to obtain knowledge. However, attending classes is still one of the best ways of learning. In-depth learning of advanced theories is possible only in classrooms. As more students lose interest in attending classes, it has become harder to keep their attendance healthy and at the same time, it has become more crucial to maintain their attendance records. Traditional attendance recording is a manual procedure, in which the teachers are obliged to call names and create entries on a piece of paper based on the students' responses. This procedure is susceptible to human-made mistakes and other unintentional errors. One major problem of this traditional method is proxy attendance, in which a student doesn't come to the class but secures his/her attendance entry through another person (typically, a friend or classmate). Another problem is the risk of the attendance documents being torn, damaged or lost. This paper proposes the adoption of IoT based biometric attendance logging which tries to address these problems. Fingerprint verification ensures the authenticity of attendance entries and IoT enables attendance records to be uploaded instantly to a remote web server and thus makes them safe from the aforesaid mishaps. Therefore, IoT based attendance logging using fingerprint recognition is efficient, hassle-free and less time-consuming.

II. RELATED WORKS

Using fingerprints to identify people is not a new idea at all. Fingerprints have been extensively used in criminology and forensics from long ago. One of the world's largest fingerprint recognition systems is the *Integrated Automated Fingerprint Identification System* (IAFIS), maintained by the United States Federal Bureau of Investigation (FBI) since 1999. However, the idea of using fingerprints to log attendance of students, is relatively new. The development in this field is largely associated with the breakthroughs in sensor

2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1272-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICICCS51141.2021.9432113

technology, which has resulted in the mass production of small, low-cost and accurate sensors. Several automated attendance systems have been designed and developed ever since.

Vikas Yadav and G. P. Bhole, in their paper, discussed about a cloud-based smart attendance system consisting of a Raspberry Pi 3, a GT-511C3 fingerprint sensor, a keypad and a 16x2 LCD [1]. Gopinath Sittampalam and Nagulan Ratnarajah, in their paper, proposed an IoT based solution for smart attendance management in universities, consisting of a WEMOS D1 development board, a FPM10A optical fingerprint sensor, a real-time clock module and a 16x2 LCD [2]. M.A. Meor Said et al., proposed a local server-based wireless fingerprint management system made up of a fingerprint sensor, a PIC16F876A microcontroller and XBEE modules which maintain communication with the server PC [3]. A similar wireless fingerprint system was developed by Zhang Yongqiang and LIU Ji. They used an Atmel AT89C5122 microcontroller, a fingerprint sensor and PTR2000+ modules to maintain communication with a local server [4]. Victor Oluwatobiloba ADENIJI et al., also proposed a local server-based class attendance register system consisting of a DigitaPersona U.are.U 4500 fingerprint reader and a PC. The PC contains a server application written in C# and ASP.NET [5]. Narra Dhanalakshmi et al., in their paper, proposed a biometric attendance system consisting of a fingerprint sensor, an Atmel SAMA5D31 microcontroller and a SIMCOM5360E GPRS/GSM module to communicate with a remote webserver [6]. A biometric smart attendance kit was proposed by Fahad-Bin-Mazhar et al. They used a GT-511C3 fingerprint sensor, a DS1307 RTC module and an Atmel ATmega2560 microcontroller, which processes all the attendance records and saves them to a SD card [7]. Dhiman Kumar Sarker et al., in their paper, proposed a local server-based smart attendance management system consisting of an Arduino Mega 2560, a RFID reader, a 4x4 keypad module, a GT5111C1R fingerprint sensor and a 16x2 LCD [8]. Another local-server based enhanced biometric attendance system was developed by Happy N. Monday et al. They used a SecuGen Hamster fingerprint reader for biometric authentication and the Java programming language to develop a server program [9]. Yash Mittal et al., in their paper, proposed biometric authentication-based access control and class attendance management systems. They used ZKTeco F19 fingerprint reader and an Arduino Uno [10].

III. METHODOLOGY

ONGULANKO is comprised of various functional blocks, of which, fingerprint verification is the most intricate and vital. The correct recognition of fingerprints is mandatory for materializing fingerprint verification. In order to recognize a particular fingerprint, there are certain fingerprint features that need to be extracted and stored in a database. A test fingerprint can be then matched against the database fingerprints to obtain the identity of that particular fingerprint.

A. Fingerprint Features

A fingerprint is basically the imprint of epidermal lines on the surface of a fingertip. These epidermal lines are called ridges. Spaces between ridges are called valleys.

Fig. 1: Ridges and Valleys.

There are three levels of features of a fingerprint which are processed for recognition: Level 1, Level 2 and Level 3. Level 1 features depict the overall layout of a fingerprint, e.g., a whorl, loop or arch. Although, this level of features cannot be used to distinguish between fingerprints, it helps narrowing down the search.

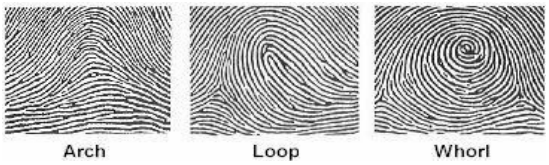

Fig. 2: Fingerprint Patterns.

Level 2 features depict specific friction ridge trails on the epidermis layer, i.e., arrangement of the friction ridges and major ridge deviations, e.g., scars, bifurcations, ridge endings, lakes, islands, incipient ridges etc. These ridge characteristics are called minutiae.

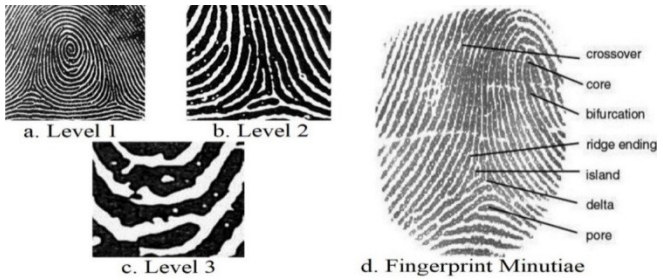

Fig. 3: Fingerprint Features & Feature Levels.

Level 3 features depict the innate details present in a developed fingerprint, such as, pores, edge details, ridge units etc. Extracting these features requires very high-resolution sensors (~1000 Dots Per Inch). ONGULANKO employs Level 2 features for reducing fingerprint template size, which reduces space complexity and subsequently the overall computational complexity.

B. Feature Extraction

Several feature extraction methods have been invented over the years, which can be roughly divided into 4 categories [11]. The first category extracts minutiae directly from the grayscale image [12, 13] without using binarization and thinning techniques, while the second category extracts minutiae from binary image patterns [14, 15]. The third category of methods uses machine learning [16, 17] for minutiae extraction and the fourth category extracts minutiae from binary skeletons [18, 19]. ONGULANKO uses the second category of feature extraction methods, in which, a fingerprint image is converted to grayscale after being captured and then it is binarized. The ridges in the binarized image are then thinned and finally the false minutiae are removed.

The process through which an enhanced grayscale image is converted into a binary image is called Binarization. A binary image contains only black and white pixels and is used for fingerprint feature detection. The concerned image is divided into black and white pixels considering the gray-level of pixels and a threshold value, which is determined using the histogram of the image.

Ridge thinning is a process by which redundant pixels are systematically removed until each ridge is just one pixel thick.

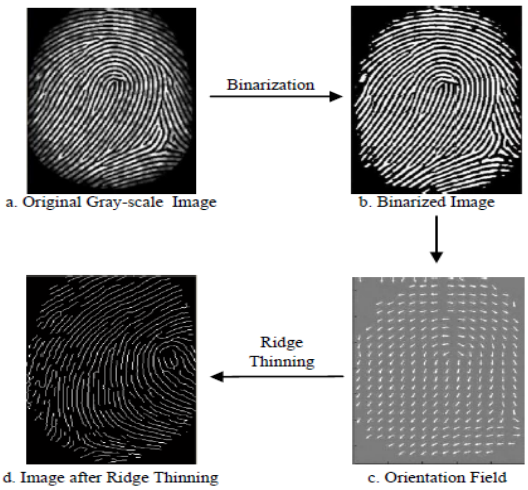

Fig. 4: Binarization and Ridge Thinning.

False removal is the post-processing required for the removal of false or spurious minutiae detected in the highly corrupted regions. False minutiae can be introduced by previous processing stages, e.g., ridge thinning. False removal includes the exclusion of short ridges, minutiae in noisy regions, and the minutiae in ridge breaks using ridge orientations.

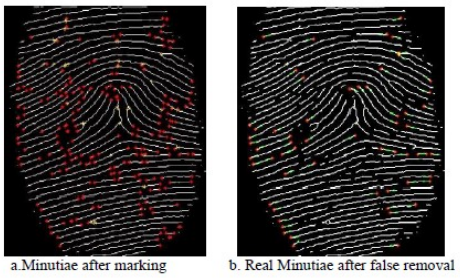

Fig. 5: False Minutiae Removal.

After removal of false minutiae, the final image is saved in a database.

C. Fingerprint Matching

ONGULANKO employs feature-based fingerprint matching, where minutiae, e.g., ridge ending, bifurcation etc., are extracted from a database fingerprint image and a test fingerprint image, and the number of corresponding minutiae pairings between the two images is used for identifying the test fingerprint. If the number of pairings exceeds a certain threshold value (set by the programmer), the test fingerprint is considered as a known fingerprint (match found) and the ID number of the fingerprint is returned, else, the test fingerprint is matched against succeeding database fingerprints and if the test fingerprint doesn't match with any of the database fingerprints, then it is considered unknown (no match found).

D. System Algorithm & Organization

There are two main modes of operation of the system; Registration and Attendance Recording. A new student's fingerprint is recorded and registered on the database through Registration mode, while, daily attendance logging of a particular course/class is materialized through the Attendance Recording mode. After booting up, the system will ask for the remote server's URL, which enables the prototype to be used with different servers of different institutions. After that, the user will be asked to select his/her preferred mode of operation (e.g., Attendance Recording, Registration). In Registration/Enrollment mode, a student's institutional ID is taken at first and then a new On-Device ID is taken from the remote server and then the student's fingerprint is taken two times and the two fingerprints are matched against each other to ensure the maximum extraction of fingerprint features. If the fingerprints match with each other, the features are extracted and stored in the device's database and subsequently the fingerprint template and ID is uploaded to the remote server's database. This process goes on and on until the device is reset.

In Attendance Recording mode, class/course name is taken from the user at first and then it is cross-checked with the remote server's class database. If the class/course exists on the

remote database, the device advances to capturing fingerprints. One by one, all the fingerprints of students of a particular course/class is taken and matched against the device database fingerprints. If a student's fingerprint matches with a fingerprint in the device's database, the ID of that fingerprint is uploaded to the remote server's database. However, if that student is not registered for that particular course/class, his/her attendance entry will be ignored by the custom-built web app of ONGULANKO [20].

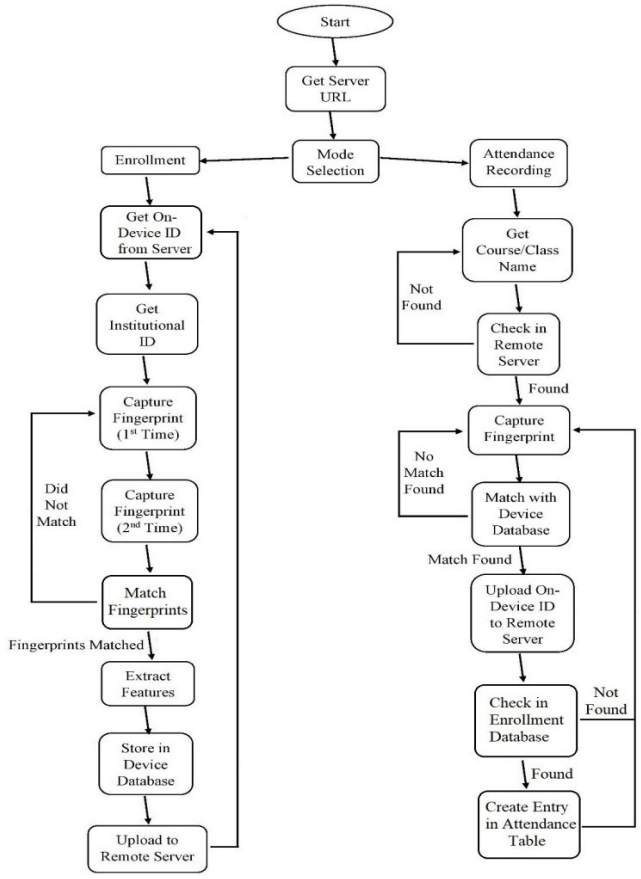

Fig. 6: System Algorithm Flowchart.

For smooth input/output operations, two separate applications were developed, one of them is an Android app and the other one is a web app. The Android app takes all the inputs (e.g., Institutional ID, Class/Course Name, Operation Mode etc.) from the user, instructs the user on how and when to give his/her fingerprint and also notifies about important events (e.g., match found/not found etc.).

The web app of ONGULANKO manages and displays all the attendance, enrollment and class/course records. There are four main pages in the web app; Login, Attendance Records, Classes and Students. From the Login page, system administrators and teachers can log in the system using their credentials and create/alter records according to their needs. Attendance records can be viewed, deleted, modified and downloaded as a CSV file from the Attendance Records page. The records can be filtered by Class/Course, Institutional ID and Date. Classes/courses can be viewed, created, copied and deleted from the Classes page. Adding students to a particular class can also be done through this page. All the registered students and their fingerprint templates can be viewed from the Students page.

There are two types of ID numbers used in the system. The first one is the On-Device ID, which is basically an integer. It is used for identifying the fingerprints on the device database. The other one is the Institutional ID, which is a string. The ID numbers used in different educational institutions are often complicated and have many segments. These segments are basically identifiers, i.e., these represent different types of information (admission year, semester, batch, roll etc.) regarding a particular student. For instance, student IDs at Daffodil International University, consist of three segments, e.g., 192-15-13154. For this reason, Institutional IDs are introduced and kept in a separate table on the remote server's database. This table contains both On-Device and Institutional IDs and the correspondence between the two.

devid	orgid	hex
1	192-15-13154	FFFFFFFFFFFFFFFFF0166148100FFFEFC7E80060000000000...
2	192-15-13155	FFFFFFFFFFFFFFFFF01591C8000F00EC002C0008000000000...

Fig. 7: ID Correspondence Table.

All the class/course records are kept in a separate table on the remote server's database. Student IDs of a particular class/course can be copied entirely or selectively to a new class. If all of the students of a particular class/course get promoted to higher class/course, then the old class/course information can be copied to the new class/course. This increases the overall ease-of-use of ONGULANKO.

	classid	classname
Edit Copy Delete	6	CSE111/A/FALL19

Fig. 8: Classes Table.

There is a separate table for keeping class/course enrollment information as well. A student can be enrolled in multiple courses in a semester and also throughout his/her university life, keeping an enrollment table enables the students to provide their fingerprint only once in their entire academic life. They can be added to and removed from various class/courses very easily afterwards.

	classid	devid
Edit Copy Delete	6	1
Edit Copy Delete	6	2

Fig. 9: Enrollment Table.

The enrollment table has been implemented using relational database. Student On-Device IDs and class/course IDs kept in this table are linked with respectively On-Device IDs in the students table and class/course IDs in the class/course table. If any student information is changed in the students table, it is automatically updated in the enrollment table. This helps to add a particular student to a particular course/class and also maintain consistency of information in the system.

IV. Electronic Components

A few hardware components are required to materialize the proposed system. First, an appropriate fingerprint sensor is required for implementing biometric authentication. The *R307* fingerprint module [21], which consists of an optical fingerprint sensor, a high-performance digital signal processor and high-capacity flash memory are used. The module is very lightweight and portable. It exhibits astounding power efficiency as it requires only 50mA of current during normal usage. It can capture images of up to 500 DPI resolution and store 1000 fingerprints on its memory. The False Acceptance Rate (FAR) and False Rejection Rate (FRR) of this module are respectively 0.001% and < 1.0%. The image processing, feature extraction and matching algorithms are all integrated in the module. The module can communicate with PCs/MCUs though the Universal Asynchronous Receiver-Transmitter (UART) protocol and features 1:1 matching/comparison and 1:N search method.

The optical sensor (CCD) in *R307* captures fingerprints using the principle of Frustrated Total Internal Reflection (FTIR).

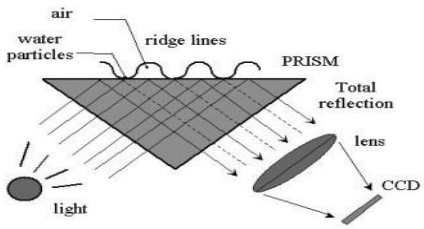

Fig. 10: FTIR Based Fingerprint Capture.

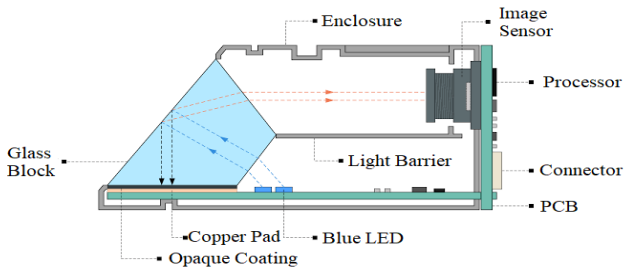

Fig. 11: R307 Cross Section.

Next, we need a processor for data collection and processing of those data. In other words, we need a brain for the system. The brain of ONGULANKO is the microcontroller *Espressif ESP8266*, which features a *Tensilica L106* 32-bit RISC processor capable of achieving extra-low power consumption and a maximum clock speed of 160 MHz. A *NodeMCU v2* [22] has been used in order to utilize this microcontroller and program it easily.

Fig. 12: NodeMCU v2.

We also need a communication link between our Android app and our prototype. For this purpose, we used the *HC-05* [23] Bluetooth module. It is a low-cost, lightweight, compact and reliable module which follows the IEEE 802.15.1 Bluetooth standard. It supports Serial Port Profile (SPP) and Universal Synchronous and Asynchronous Receiver-Transmitter (USART) protocol, which are used for communicating with PC. It is also Transistor-Transistor Logic (TTL) compatible, which makes interfacing with microcontrollers extremely convenient. It has an operating voltage of 4-6V and requires only 30mA of current during normal usage. It has a range of ~10m and a maximum baud rate of 460800 bauds per second.

Fig. 13: HC-05 Front (Right) & Back (Left) View.

Since all of the hardware components run on 5V, we used a custom-built 5V rechargeable power supply to power the hardware. Two 3.7V Lithium-Ion battery cells, each having a capacity of 1000 mAh, were used in parallel in the power supply. The 3.7V of the batteries is stepped-up in the Battery Management System (BMS) [24]. The BMS can deliver up to 1A of current at any instance. It also offers short-circuit, under-voltage and over-voltage protection, which keeps the electronics and battery cells safe.

There is an on-board voltage regulator on the BMS, which provides steady 5V on the output, so additional voltage regulation wasn't necessary. The hardware, in average, consumed a total of 125mA of current. The used power supply was fluent in handling the load. We tested the supply and found that it is capable of running the system for 16 hours straight. After 16 hours, the BMS cuts the power off automatically to protect the battery cells from over-discharging.

V. SOFTWARE AND COMMUNICATION

The *NodeMCU* was programmed using the PlatformIO IDE [25]. Lua is *NodeMCU*'s official programming language, however, C++ was used for simplicity and efficiency. After booting up, the NodeMCU automatically connects to a pre-defined access point (Wi-Fi router) and then waits for a Bluetooth device (smartphone) to connect to it. After a Bluetooth client has been connected, the device asks the user for his/her preferred mode of operation (Enrollment, Attendance Recording, Deletion) though the Android app. In Enrollment mode the device takes Institutional IDs and corresponding fingerprints. The fingerprints are saved in the device's memory and template hex codes and IDs (On-Device and Institutional) are uploaded to the remote server. In Attendance Recording mode, the fingerprint module captures fingerprints, matches them with the device database and returns On-Device IDs if matched and these IDs are then uploaded to the remote server. While uploading IDs and templates, an URL string is formed every time, which contains these IDs, hex codes, and the URL is accessed by utilizing the HTTP GET method [26]. We used Transmission Control Protocol (TCP) for secure and reliable data transmission. The webserver contains several PHP scripts that receive data from the *NodeMCU* in real-time and store the data into a pre-built MySQL database. The web app of ONGULANKO was written in HTML and beautification was done using CSS, specifically, the Bootstrap framework [27]. jQuery [28] and AJAX [29] were used in order to update elements on webpages as soon as data is updated in the database, without having to refresh entire pages. When first accessed, the web app of ONGULANKO will ask for username and password, which can be collected from the system administrators.

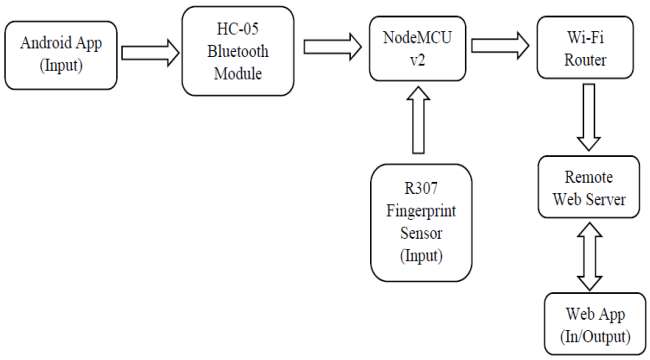

Fig. 14: Data Flow Path of ONGULANKO.

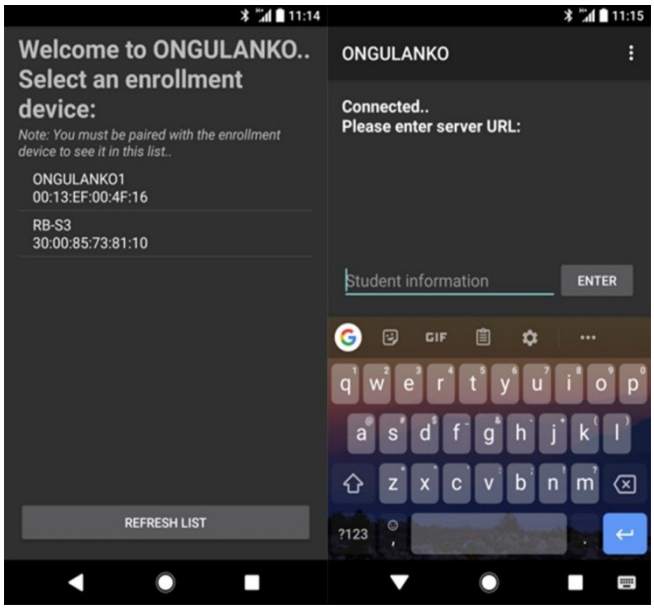

Fig. 15: Android App's Device Selection Screen (Left) & Home Screen (Right).

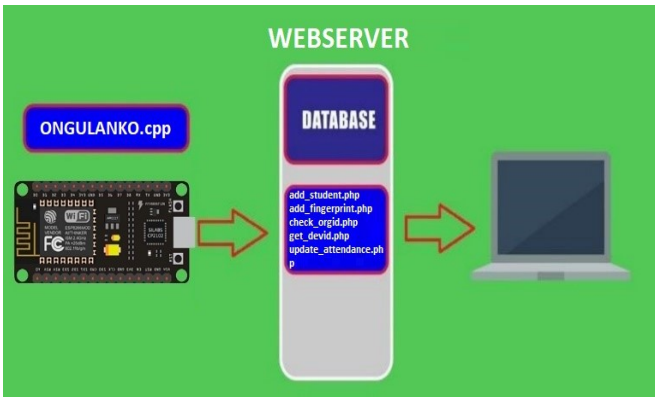

Fig. 16: Backend Mechanism.

VI. RESULTS AND COMPARATIVE ANALYSIS

The system was rigorously tested to ensure proper functionality in the actual field. 10 groups, each containing 10 students, were registered on the system and their attendances were taken. The results can be found in Table 1.

TABLE I. ENROLLMENT AND ATTENDANCE RECORDING TEST RESULTS

Group No.	Enrollment		Attendance Recording	
	False Acceptance	False Rejection	False Acceptance	False Rejection
01	00	01	00	01
02	00	02	00	01
03	00	00	00	00
04	00	01	00	00
05	00	00	00	00
06	00	01	00	00
07	00	00	00	00

08	00	00	00	00
09	00	02	00	00
10	00	00	00	00

As seen in Table 1, ONGULANKO showed success scenarios when tested. While enrolling a new student, there were 7 unsuccessful tries among 100 attempts. All of them were due to sweaty fingers of the students. The *R307* optical fingerprint sensor is vulnerable to sweaty/dirty fingers, and as a result, the two fingerprints taken for enrollment did not match in case of students with sweaty skin. There were no cases of false acceptance. So, the success rate while enrolling a new student is 93%. In case of attendance recording, there were only 2 failed attempts among 100 attempts, again owing to sweaty fingers. So, the success rate in this case is 98%.

TABLE II. TIME REQUIREMENT COMPARISON

Attendance System	Number of Students	Total Execution Time (Seconds)	Average Execution Time (Seconds)
ONGULANKO	50	105.7	2.11
Name/ID Calling Based	50	220.2	4.40
Victor Oluwatobiloba ADENIJI et al.	50	437.11	8.7
Attendance Sheet Based	50	733.8	14.6

The time required for recording attendance with ONGULANKO largely depends on the internet connection and the server location. The fingerprint recognition process takes less than 0.1 second, if the finger is placed correctly on top of the sensor. A propagation delay of 179 milliseconds is obtained from Dhaka, Bangladesh to our server at the United States with a 512 Kbps connection. So, it takes less than a second for the fingerprint recognition and the device-server communication processes (sending request to the server and receiving the response) to finish. The most time-consuming part was the passing of the device among the students.

Fig. 17: Hardware of ONGULANKO.

A comparison between ONGULANKO and other similar systems can be found in Table 3.

TABLE III. FEATURE COMPARISON BETWEEN ONGULANKO AND OTHER SIMILAR SYSTEMS

System Name/Authors	Adding New Class/Course	Copying Students Between Classes	Fingerprint Template Upload to Server	Self-Retry in Case of Error	Records Filter	Duplicate Entry Blocking	Course/Class Registration Check
Vikas Yadav et al. [1]	No	No	No	No	No	No	No
Gopinath Sittampalam et al. [2]	No	No	No	No	No	No	No
M.A. Meor Said et al. [3]	No	No	No	No	No	No	No
Zhang Yongqiang et al. [4]	No	No	No	No	No	No	No
Victor Oluwatobiloba ADENIJI et al. [5]	No	No	No	No	No	No	No
Narra Dhanalakshmi et al. [6]	No	No	No	No	No	No	No
Fahad-Bin-Mazhar et al. [7]	No	No	No	No	No	No	No
Dhiman Kumar Sarker et al. [8]	No	No	No	No	No	No	No
Happy N. Monday et al. [9]	No	No	No	No	No	No	No

Yash Mittal et al. [10]	No	No	No	No	No	No	No
ONGULANKO	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

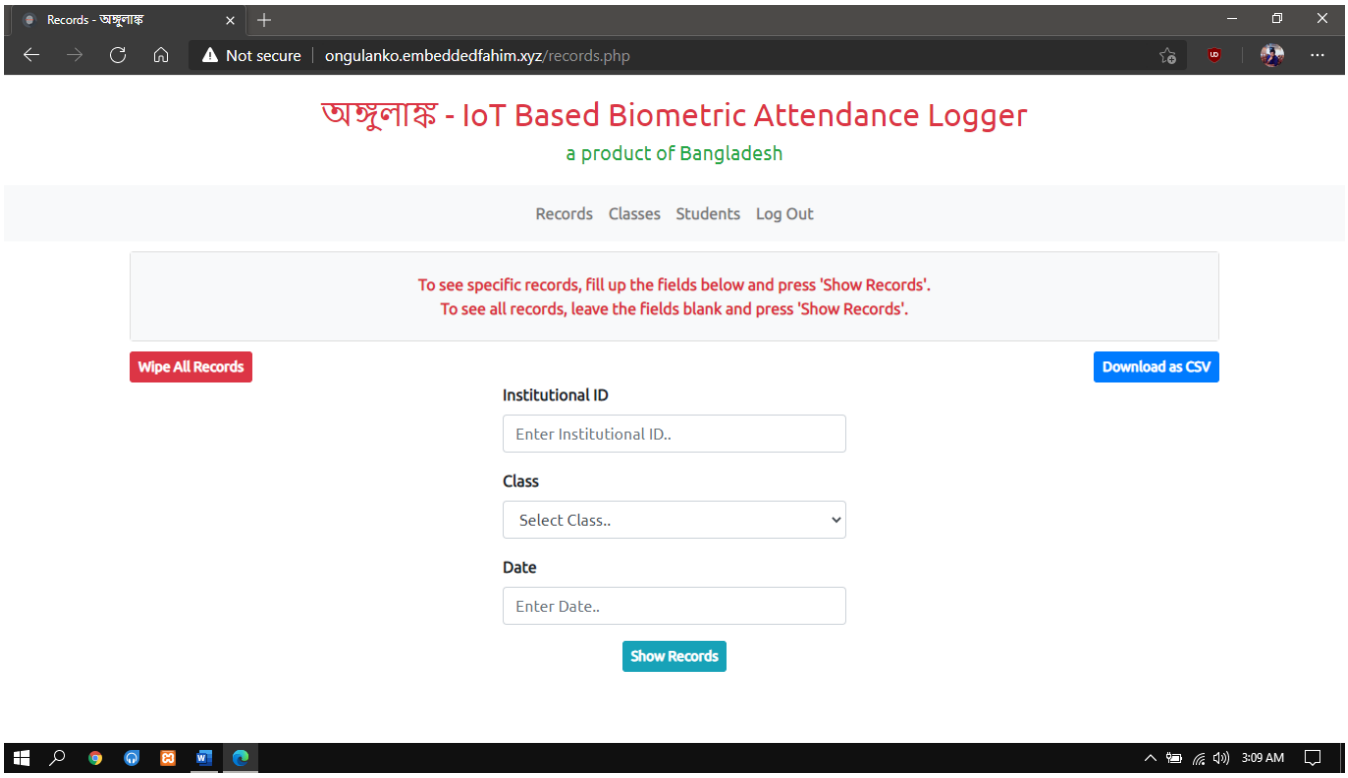

Fig. 18: Attendance Records Page of ONGULANKO's Web App.

VII. Advantages of Ongulanko

ONGULANKO is extremely portable and light-weight, weighing only 157 grams. We found the battery to last a week on a single charge with moderate use. The hardware is inexpensive, costs around 23 USD only. Both the web app and Android app instructs the user on how to use the system. The system algorithm ensures duplicate entry blocking at all stages. The *R307*'s firmware recognizes registered fingerprints in less than 0.1 second.

VIII. Areas of Further Development

Since, only a prototype of the proposed system is built, there is still room for improvements. The first improvement can be the implementation of remote/server matching, in which, the device will send the fingerprint template hex to the server and the matching will be done remotely, i.e., the test fingerprint will be matched against the fingerprints stored on the remote server. Implementing this will allow students registered on a particular device to be recognized by other devices. However, adding this feature will first require another improvement: fingerprint database sharing across multiple devices. This will allow all the devices to collect fingerprints and store them all in one place. This will also enable duplicate registration blocking, i.e., one student will only be able to register him/herself only on one device. If he/she tries to register on more than one device, the enrollment will be blocked by the server. Another improvement can be the substitution of the fingerprint sensor. Currently, the sensor used in ONGULANKO is an optical sensor. These sensors are known for false rejection, specially, in case of sweaty skin. Switching to a capacitive or ultrasonic sensor can reduce the amount of false rejection. Also, the current sensor's firmware doesn't block previously enrolled fingerprints and allows a fingerprint to be registered more than once with different On-Device IDs. With some minor modifications, the system can also be used in workplaces and other institutions which require regular attendance monitoring.

IX. Conclusion

Internet of Things opens doors to numerous possibilities by rendering real-time information over the internet. This paper attempts to demonstrate the convenience of Internet of Things in making the attendance recording procedure automated, smart and efficient. Traditional method of attendance recording is time-consuming and monotonous. To counter the problems of traditional attendance recording methods, this paper proposes the adoption of IoT based biometric attendance logging which will save a lot of valuable time and effort, while simultaneously preventing

impersonation or proxy attendance. A fully functional prototype of the system was successfully developed. Fingerprints were taken through the prototype and students were successfully registered on the system and their attendance was also taken, which was then displayed on the system's website. Since attendance data is stored in the cloud, it becomes less vulnerable to data loss and easier to fetch, use and re-use. It makes the process of attendance recording convenient for both the students and teachers. It also makes the management of attendance data easier for institutions.

ACKNOWLEDGEMENT

The authors of this paper are very much grateful to the faculty members of the Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh, for their encouragement throughout the build of this project. Without their support, this research work could never pursue such a complicated project.

REFERENCES

[1] V. Yadav and G. P. Bhole, "Cloud Based Smart Attendance System for Educational Institutions," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 97-102, DOI: 10.1109/COMITCon.2019.8862182.

[2] G. Sittampalam and N. Ratnarajah, "SAMS: An IoT Solution for Attendance Management in Universities," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 251-256, DOI: 10.1109/TENCON.2019.8929616.

[3] M. A. Meor Said et al., "Biometric attendance," 2014 International Symposium on Technology Management and Emerging Technologies, Bandung, 2014, pp. 258-263, DOI: 10.1109/ISTMET.2014.6936516.

[4] Z. Yongqiang and L. Ji, "The Design of Wireless Fingerprint Attendance System," 2006 International Conference on Communication Technology, Guilin, 2006, pp. 1-4, DOI: 10.1109/ICCT.2006.341990.

[5] V. O. Adeniji, M. S. Scott and N. Phumzile, "Development of an Online Biometric-enabled Class Attendance Register System," 2016 IST-Africa Week Conference, Durban, 2016, pp. 1-8, DOI: 10.1109/ISTAFRICA.2016.7530647.

[6] N. Dhanalakshmi, S. G. Kumar and Y. P. Sai, "Aadhaar Based Biometric Attendance System Using Wireless Fingerprint Terminals," 2017 IEEE 7th International Advance Computing Conference (IACC), Hyderabad, 2017, pp. 651-655, DOI: 10.1109/IACC.2017.0137.

[7] Fahad-Bin-Mazhar, O. Ahamed and M. Rasedujjaman, "Biometric smart attendance kit with fingerprint scanner by using microcontroller," 2015 International Conference on Electrical & Electronic Engineering (ICEEE), Rajshahi, 2015, pp. 13-16, DOI: 10.1109/CEEE.2015.7428261.

[8] D. K. Sarker, N. I. Hossain and I. A. Jamil, "Design and implementation of smart attendance management system using multiple step authentication," 2016 International Workshop on Computational Intelligence (IWCI), Dhaka, 2016, pp. 91-95, DOI: 10.1109/IWCI.2016.7860345.

[9] H. N. Monday, I. D. Dike, J. P. Li, D. Agomuo, G. U. Nneji and A. Ogungbile, "Enhanced attendance Management System: A Biometrics System of Identification Based on Fingerprint," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2018, pp. 500-505, DOI: 10.1109/IEMCON.2018.8614776.

[10] Y. Mittal, A. Varshney, P. Aggarwal, K. Matani and V. K. Mittal, "Fingerprint biometric based Access Control and Classroom Attendance Management System," 2015 Annual IEEE India Conference (INDICON), New Delhi, 2015, pp. 1-6, DOI: 10.1109/INDICON.2015.7443699.

[11] R. C. Gonzalez and R. E. Woods., Digital Image Processing, Prentice Hall, Upper Saddle River, NJ, 2002.

[12] Jinxiang Liu, Zhongyang Huang and Kap Luk Chan, "Direct minutiae extraction from gray-level fingerprint image by relationship examination," Proceedings 2000 International Conference on Image Processing (Cat. No.00CH37101), Vancouver, BC, Canada, 2000, pp. 427-430 vol.2, DOI: 10.1109/ICIP.2000.899435

[13] Bir Bhanu and Xuejun Tan, "Fingerprint indexing based on novel features of minutiae triplets," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 5, pp. 616-622, May 2003, DOI: 10.1109/TPAMI.2003.1195995.

[14] R. S. Germain, A. Califano and S. Colville, "Fingerprint matching using transformation parameter clustering," in IEEE Computational Science and Engineering, vol. 4, no. 4, pp. 42-49, Oct.-Dec. 1997, DOI: 10.1109/99.641608.

[15] Wu, Chaohong & Shi, Zhixin & Govindaraju, Venu, "Fingerprint image enhancement method using directional median filter," Proceedings of SPIE - The International Society for Optical Engineering, 2004, DOI: 10.1117/12.542200.

[16] Prabhakar, Salil & Jain, Anil & Pankanti, S., "Learning Fingerprint Minutiae Location and Type", Pattern Recognition, Volume 36, Issue 8, 2003, pp. 1847-1857, DOI: 10.1016/S0031-3203(02)00322-9.

[17] V. K. Sagar, D. B. L. Ngo and K. C. K. Foo, "Fuzzy feature selection for fingerprint identification," Proceedings of The IEEE 29th Annual 1995 International Carnahan Conference on Security Technology, Sanderstead, Surrey, UK, 1995, pp. 85-90, DOI: 10.1109/CCST.1995.524738.

[18] A. Jain, Lin Hong and R. Bolle, "On-line fingerprint verification," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 302-314, April 1997, DOI: 10.1109/34.587996.

[19] Feng Zhao, Xiaoou Tang, "Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction," Pattern Recognition, Volume 40, Issue 4, 2007, pp. 1270-1281, ISSN 0031-3203, DOI: 10.1016/j.patcog.2006.09.008.

[20] "Web App of ONGULANKO," Last accessed on February 1, 2021, at 12:00:00 PM [Online]. Available: http://ongulanko.embeddedfahim.xyz

[21] "R307 Fingerprint Sensor," Last accessed on February 1, 2021, at 12:05:00 PM [Online]. Available: https://www.sunrom.com/p/finger-print-sensor-r307-new-r305

[22] "NodeMCU v2," Last accessed on February 1, 2021, at 12:10:00 PM [Online]. Available: https://www.seeedstudio.com/NodeMCU-v2-Lua-based-ESP8266-development-kit.html

[23] "HC-05 Bluetooth Module," Last accessed on February 1, 2021, at 12:15:00 PM [Online]. Available: https://components101.com/wireless/hc-05-bluetooth-module

[24] "Battery Management System," Last accessed on February 1, 2021, at 12:20:00 PM [Online]. Available: https://www.electronics.com.bd/5v-1a-power-bank-charger-module-charging-circuit-board-step-up-boost-power-module

[25] "PlatformIO," Last accessed on February 1, 2021, at 12:25:00 PM [Online]. Available: https://docs.platformio.org/en/latest/

[26] "HTTP GET Method," Last accessed on February 1, 2021, at 12:30:00 PM [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods

[27] "Bootstrap," Last accessed on February 1, 2021, at 12:35:00 PM [Online]. Available: https://getbootstrap.com/docs

[28] "jQuery," Last accessed on February 1, 2021, at 12:40:00 PM [Online]. Available: https://api.jquery.com/

[29] "AJAX," Last accessed on February 1, 2021, at 12:45:00 PM [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/Guide/AJAX/Getting_Started