INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Portable biometrics using LoRa modulated interface

Bharath K.
bharathk59@gmail.com
Dr. Ambedkar Institute of Technology, Bengaluru, Karnataka

Bhargava U. G.
bhargavaug97@gmail.com
Dr. Ambedkar Institute of Technology, Bengaluru, Karnataka

Girija S.
girija.s@dr-ait.org
Dr. Ambedkar Institute of Technology, Bengaluru, Karnataka

ABSTRACT

Many of the universities in India has always been facing issues with its students' attendance registry management and thereby wasting valuable manpower and time for the faculties of the institutions. There have also been some standalone biometric devices which are rather costly, as well as non-portable and people can tamper with them. These problems are overcome by using a portable device which checks the validation of the unique characteristics (fingerprint) of the subject if it is a valid input, and then it will store the data of the subject's presence in the Excel spreadsheet in the faculty's personal computer and report the success. The data (ID of the student) will be sent through an LPWAN communication protocol called LoRa. This way there will be complete safety of the data, as it will not be tampered (in case of standalone devices, which can be tampered with) and the complete information is stored in the central database. The automatic logging greatly reduces the task carried out by the faculties at the end of the semesters since the data is readily available and required action can be taken concurrently.

Keywords— *LoRa, Modulation, Attendance management, Arduino, Fingerprint*

1.INTRODUCTION

In the Indian education system, student attendance system plays a major role in the teaching and learning process. In most of the Universities, student attendance is taken manually in the attendance sheet and then after it is being processed by data entry operator or online attendance system. Both of these methods are time-consuming and error prone as the attendance details are entered and maintained by human beings. In an institution, the average student count in one classroom is 60. Students have to mark their attendance in every hour. Using conventional methods like callout for students' names for attendance will take approximately 5 or 10 minutes to complete the process for a class. If there are 7 classes per day and if we consider that the class is for one hour, approximately 6 hours in a week is used for marking attendances. This is a total waste of manpower and precious lecturing time.

The main objectives of this paper are:

- To solve the issue of inefficient attendance marking systems by relying on modern communication technique.
- To reduce the unwanted efforts made by faculty, with which they can concentrate on the academics.

2.RELATED WORKS

Today, biometric is being spotlighted as the authentication method because of the need for reliable security. 80% of the public has biometric recorded. Thus, it is very well accepted in the government and also in the private sectors for better security. It has a long history in judicial science, complete with many studies which back up the use of fingerprints for identification. Fingerprint identification is widely understood as highly accurate means and very trustworthy process since the statistical chance of two people on Earth having identical fingerprints is very low. Previously significant work has been done regarding academic attendance monitoring problem. In the 14th century, a European explorer by name Joao de Barros had the earliest recorded example of fingerprinting, which is a form of biometrics. Chinese merchants had used a type of ink to take people's fingerprints for identification purpose. Recently, Oloyede et al. (2013) had carried out research on the application of biometric technology to solve the problem of staff attendance. However, these researchers did not provide any software to address the problems of attendance [1].

Similarly, Derawi et al. (2012) also proposed a method to implement cell phone cameras for capturing fingerprint images and later on evaluate up to 1320 fingerprint images from a type of embedded capturing devices. He had used a Nokia N95[2] as the mentioned device. The results proved that an equal error rate (EER) of 4.5% can be achieved.

Also, Sin et al. (2012) proposed a target structure system for fingerprint verification where templates of fingerprints were replaced with matching. The system presented an ERR of 2% after updating the evaluation [3].

Some faculty members use the signature method for attendance marking. Many organizations use a fingerprint attendance system for marking attendances of their employees using non-portable devices connected to computers with the database. But the situation in the classroom is different. The students may have to change the classrooms every hour to attend different

lectures and attendance will be taken for every lecture. Hence, these approaches to wired connection systems will not be useful. The concept of wireless fingerprint attendance system has since been proposed by several research groups.

L. Jian-Po et al. developed a system using wireless technology [4]. They created a database in the remote system and the fingerprint data transmitted to the computer using ZigBee wireless technology. It could provide a range of 30 to 70 meters if there is no barrier [5]. So the students cannot use this device if the classroom is not in the range of ZigBee. Many mobile phone manufacturers have come up with various applications on their devices to facilitate the fingerprint attendance system.

Another system was developed by Saim, Arash, Azhar-ud-din and Tabassam, (2009) which would take student lectures attendance when entering the lecture rooms [6] which is a fingerprint-based model and was designed for students only. But this was a drawback as anyone could access the device present outside and can tamper with the data.

This paper provides information about how to achieve accurate fingerprint authentication as well as portable while preserving data integrity, such that the data cannot tamper. We propose a system which utilizes a Low-Power Wide-Area Network (LPWAN) which is a centralized system to achieve the said aim.

3. THEORETICAL BACKGROUND

3.1 Conventional Attendance System

The model diagram of existing attendance system is shown in Figure 1. In both methods shown, it requires user intervention to do the entry of absent number in particular session whether it is lecture or laboratory. There are flaws in these approaches:

(a) As the operator performs the entry of absentees, there can be typing mistakes and there are the chances of making false positives of attendance.

(b) A data entry operator needs to spend some time doing the entry of absent number so it is a time-consuming process.

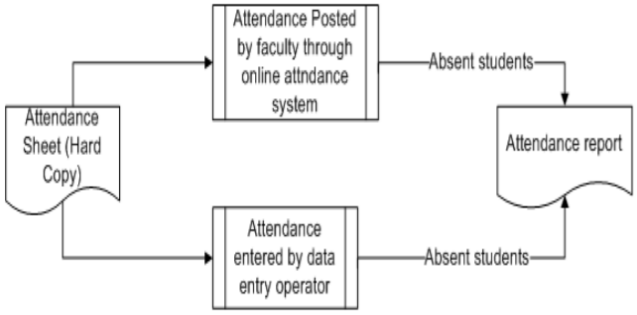


Fig. 1 Conventional attendance system representation

3.2 References to previous works

Biometric authentication is based on unique individual characteristics. There are two types of biometric authentication. Physical biometrics: includes DNA analysis, fingerprints analysis, facial recognition, and eye scans (retina and iris). Behavioural biometrics: includes handwritten signature analysis and voice recognition.

The biometric authentication process includes several stages: measurement, signal processing, pattern matching, and decision making. Measurement involves sensing biometric characteristics and is necessary both for the creation of the database and for each authentication trial. For example, when voice verification is utilized, this stage involves recording one's voice through a microphone. Then the digital data are mathematically modelled. When the user wants to be authenticated, the device compares the received data to the user model and makes a decision mostly based on a pre-calculated threshold.

The usual biometric authentication methods which use technologies like ZigBee and Wi-Fi have certain disadvantages such as low range, interference etc. Also, Standalone biometric devices are more prone to fraud, data corruption and have added disadvantage of non- portability.

3.3 LoRa Technology

LoRa is a type of chirp spread spectrum modulation [9] utilizing frequency chirps which have a linear variation of frequency over time for encoding information in it. The advantage of Chirp Spread Spectrum is that the frequency offsets are equivalent to timing offsets between transmitter and receiver because of the linearity of the chirp pulses, making this modulation immune to the Doppler Effect.

It is found that LoRa symbol duration is longer than the typical bursts of AM interference generated by Frequency Hopping Spread Spectrum systems. Hence, errors generated by interference are easily corrected through forwarding Error-correction Codes (FECs). Due to this, LoRa has better performance when compared to traditional modulation schemes, such as Frequency-Shift Keying (FSK), and makes LoRa well suited to low-power and long-range transmissions.

4. DESIGN AND METHODOLOGY

4.1 Enrolment

The task of the enrolment module is to enrol users and their fingerprints into the database (fingerprint module). During enrolment, depicted in Figure 2, the fingerprint is captured and unique features are extracted from a fingerprint image and stored in the database as a template with the user's ID mapped on to it. The process of enrolment in the database is done twice, that is the user is prompted to input their credentials twice for checking if the genuine fingerprint is being updated into the database.

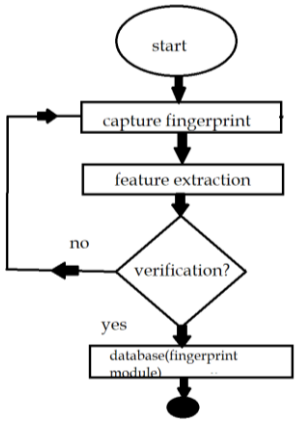


Fig. 2: Enrolment Phase Flow

4.2 Authentication

The task of the authentication is to validate the identity of the person. It is as shown in the flow diagram indicated by Figure 3. The person to be authenticated indicates his/her identity and places his/her finger on the fingerprint scanner where the scanner is in waiting for the state. The fingerprint image is captured and at the feature extraction stage, the biometric template is extracted. It is then fed to matching algorithm for verification, which matches the extracted fingerprint information against the person's biometric template stored in the database to establish identity and ID is sent through LoRa.

It is then transmitted via LoRa module to the receiver present in the backend situated at the department office, where data about the presence of the student is logged in to the systems. This is indicated by the receiver module flow diagram indicated in figure 4.

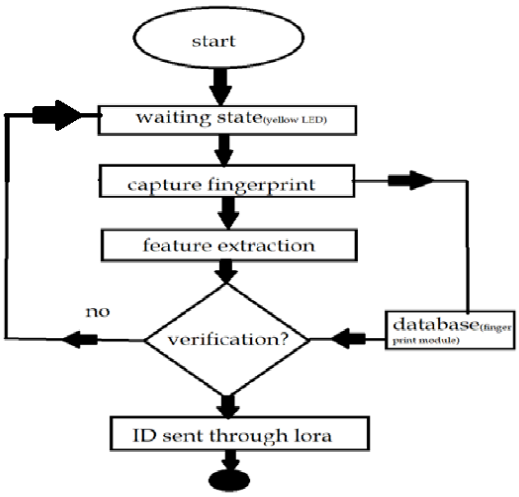


Fig. 3: Authentication Phase Flow

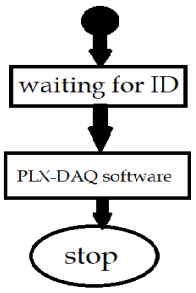


Fig. 4: LoRa Receiver Module Flow

4.3 LoRa Modulation

A communication interface is needed which covers the range more than the mentioned methods in Related works like ZigBee and Wi-Fi. Thus we utilize the technique of newly emerging Low Power Wide Area Network (LPWAN) [9] which, as the name says consumes very less power and covers a wider range. It is widely used in the communication of IoT based devices [10], to the main server to which they're connected to. This is due to three basic elements of communication namely, bandwidth, range and power. If one needs to enhance any one of the parameters, for example, Bandwidth, then the usage of the power needs to be compromised, as well as the probability of interference of the received signal.

There are many types of LPWANs among which the main focus here is the chirp spread spectrum (CSS) based LoRa. Chirp stands for 'Compressed High-Intensity Radar Pulse'. It is a signal where frequency either increases or decreases with time. It is commonly used in implementing sonar and radar and used in spread-spectrum. In telecommunication systems, spread-spectrum modulations are methods by which a signal generated with a particular bandwidth is purposefully spread in all frequencies in the frequency domain, which results in a signal having a wider bandwidth. Hence, by increasing the bandwidth of the signal, compensation for the degradation of the signal-to-noise (SNR) ratio of a radio channel is achieved.

There is a traditional Spread Spectrum technique called Direct Sequence Spread Spectrum (DSSS) systems, where the carrier phase of the transmitter will change in accordance with a code sequence. The process is achieved by multiplying the wanted data signal with a spreading code, which is called a chip sequence. This chip sequence will always occur at a faster rate than the data signal and hence will spread the bandwidth of the signal beyond the bandwidth occupied by just the original signal. The term chip is used because it becomes easy to distinguish the shorter coded bits from the longer un-coded bits of the signal.

At the receiver side, the data signal is recovered by again multiplying with a locally generated replica of the spreading sequence. This process in the receiver will effectively compress the spread signal back to its original un-spread bandwidth, The amount of spreading is dependent on the ratio of "chips per bit", which is the ratio of the chip sequence to the data rate, is referred to as the processing gain, commonly expressed in dB.

Where:
RC = Chip Rate (Chips/second)
Rb = bit-rate (bits/second)

However, challenges certainly do exist for the above-mentioned method. Some of them are a requirement of a highly accurate reference clock source which is expensive, the longer time required for correlation by the receiver for longer code. Hence, CSS is used.
Chirp Spread Spectrum was initially developed for radar applications [12]. Chirp signals have constant amplitude and pass the whole bandwidth in a linear or non-linear way from one end to another end in a certain time. They use complete bandwidth to transmit signals. If the frequency changes from lowest to highest, it is called up-chirp and if the frequency changes from highest to lowest, it is called down-chirp. Figure 5 depicts the example of linear up-chirp:

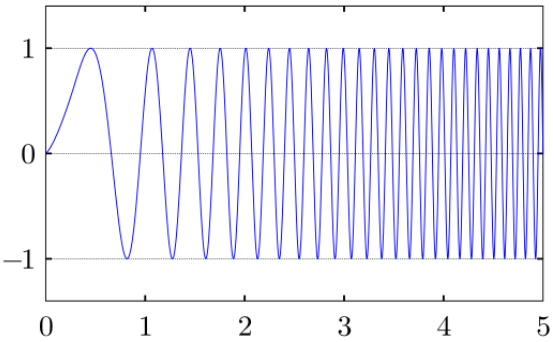


Fig. 5: Time domain representation of a linear up-chirp

There are various parameters for LoRa modulation: Bandwidth (BW), Code Rate (CR) and Spreading Factor (SF). LoRa uses a unique definition of the spreading factor as the logarithm, in base 2, of the number of chirps per symbol. These parameters influence the effective modulation, its ease of decoding and resistance to interference noise.

The bandwidth is the important parameter of the LoRa modulation. A primitive unit of LoRa signal is called as a LoRa symbol. A LoRa symbol consists of 2*SF numbers of chirps, which will cover the entire frequency band. This symbol starts with a series of upward chirps. When the maximum frequency of the band is reached, the frequency wraps around, and the process repeats again from the minimum frequency. The encoding of information takes place due to the position of discontinuity.

As there are 2*SF chirps in a symbol, a symbol can effectively encode SF bits of information.

The chirp rate is equal to the bandwidth. This has several

disadvantages like; increase in one of the spreading factor will divide the frequency span of a chirp by two and multiply the duration of a symbol by two and, one more bit will be transmitted in each symbol, hence, it will not divide the bit rate by two. This is depicted in Equation (1), which links the symbol duration (TS) to the spreading factor and the bandwidth.

$$TS = 2^{(SF/BW)} \quad (1)$$

Generally, LoRa is popular because, an increase of bandwidth lowers the receiver sensitivity, whereas an increase of the spreading factor increases the receiver sensitivity. Moreover, decreasing the code rate helps reduce the Packet Error Rate (PER) in the presence of short bursts of interference.

Although the LoRa modulation can be used to transmit arbitrary frames, a physical frame format is specified and implemented in LoRa receivers [13]. The spreading factor and bandwidth are constant for a frame.

A LoRa™ frame will begin with a preamble which symbolizes the beginning of a frame. The preamble will start with a constant up chirp sequence that covers the whole frequency band. The final two up chirps encode the synchronization word. The synchronization word is a one-byte value that is used for differentiating LoRa networks that use the same frequency bands. Hence, there will be no interference between two transmissions on the same channel. A device set with a given synchronization word will refuse to listen to transmission if the decoded synchronization word does not match its configuration. The overall duration of this preamble signals can be set between a minimum of 10.25 and maximum of 65,539.25 symbols. The structure of the preamble can be seen in figure 7.

After the preamble, there is an optional header. If not, it is followed by a payload. The payload size is stored using one byte, limiting the size of the payload to 255 bytes. The header is optional to allow disabling it in situations when not necessary, for instance, if the payload length, coding rate and CRC presence are known in advance.

A payload is sent after the header, and at the end of the frame is the optional CRC. A schematic summarizing the frame format can be seen in figure 6.

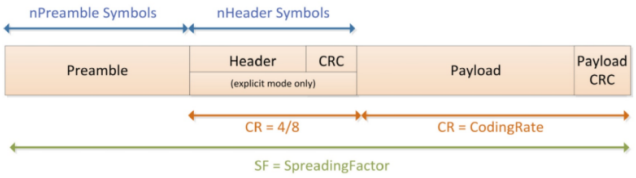


Fig. 6: Structure of a LoRa™ frame, n ∈ {1..4}

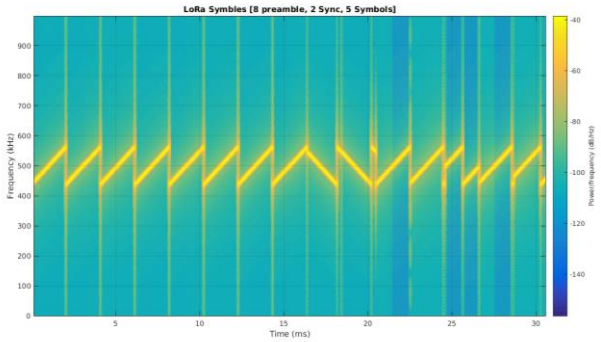


Fig. 7: Spectrogram of LoRa™ physical layer

After the preamble, Cyclic Redundancy Checksum (CRC) is produced and is included after the preamble. This makes sure that the symbols are received by the receiver without any errors, else requests to retransmit the data. After the CRC, the payload is transmitted at a rate specified by the Coding Rate (CR). Optional payload CRC can also be included. Figure 7 shows the spectrogram, visualising the frequency spectrum of the entire LoRa frame.

The LoRa system designed makes use of the unlicensed frequencies dedicated to Industrial, Scientific and Medical (ISM) bands that are available worldwide. The most widely used bands are:

1) 868 MHz for Europe
2) 915 MHz for North America
3) 433 MHz band for Asia

Using lower frequencies than those of the 2.4 or 5.8 GHz ISM bands gives much better coverage especially when the nodes are within buildings.

Some Key Properties of LoRa Modulation are Scalable Bandwidth, Constant Envelope/Low Power, High robustness, Enhanced network capacity, Doppler Shift Resistance etc. These properties make the LoRa modulation stand out from the rest of conventional modulation techniques.

5. IMPLEMENTATION

There are four major steps in implementation:

(a) Fingerprint Enrolment Phase: Student will enroll their fingerprint via the fingerprint sensor, which is the standard R307 scanner. Here, the fingerprint sensor detects and captures the fingerprint image and extracts the unique minute data. Students are then required to scan their fingerprint again and the extracted features are compared with the one taken in the previous session. If the system found the fingerprints are matched, the unique minutiae data is saved into the database as a template, with a unique number called as ID for each template stored.

(b) Authentication Phase: During authentication, the bio-metric of the student is captured during the lecture session. The captured image is compared with that stored in the database using a matching algorithm.

(c) Wireless Transmission of ID: The ID of the subjects whose attendance is taken, is sent over a wireless communication interface which acts like a radio (transmits data). The interface technology used here is called LoRa, which has a transmission range of over 10 kilometres in n line-of-sight communication. The IC used for the required operation is LoRa-RA02 transceiver modules. The IC present at the receiver end picks up the transmitted signal, which is connected to another Arduino, which puts the received ID in a new column of the Excel spreadsheet. Meanwhile LED feedbacks are given for indicating the status of the process.

(d) Data Logging Phase: During the enrolment phase a unique identification number is issued to the students this ID number is very important because during the data logging phase this unique identification number is logged into excel and a simple matching algorithm is developed to match this ID number.

Codes are written for each phase using Arduino, as the LoRa modules and the fingerprint scanner are implemented on the top of Arduino Uno Microcontroller. The language used is C++. Matching algorithm: the algorithm used in the module captures the unique ridges, split ends and the relative distance between

them for each of the fingerprints scanned and stores them as a template if the fingerprint is matched when the user is prompted to give his/her fingerprint once again.

Similarly, during the verification phase, the incoming fingerprint is scanned for their unique patterns and ridges, and compared with the templates in the FLASH Chip. The identification and conversion of the ridges split ends and the relative distance between them is done by the DSP chip present on the fingerprint sensor module. It also provides a mean to export and deletes saved measurements.

6. EXPERIMENTS AND RESULTS

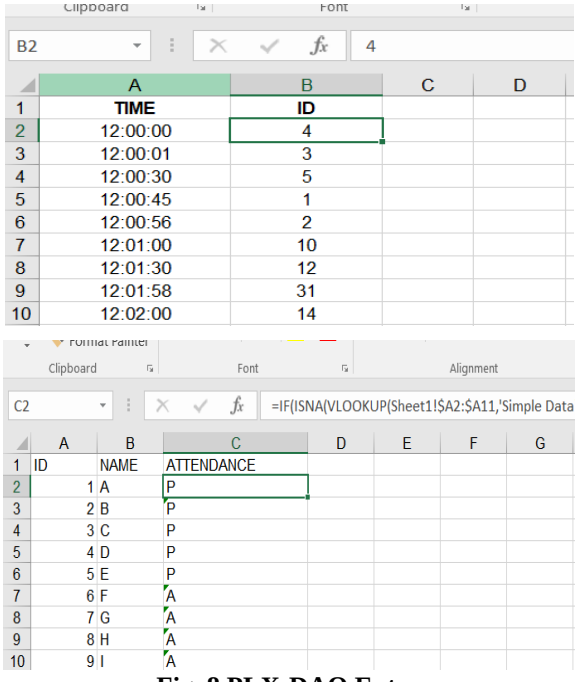
6.1 Experiment Dataset

(a) Fingerprint Creation: The student is made to enter his/her fingerprint credentials after creating an ID number for the same. The fingerprint has to be entered twice for testing the authenticity of the user's fingerprints. If the prints do not match, an error message will be displayed, returning to the initial stage. If the prints match, the terminal gives a message of the stored ID number. After collecting all students' data, the device is then ready for use in taking attendance.

(b) Fingerprint verification: The device shows an indication that it is ready to receive a fingerprint to be verified. When the input is given the finger is scanned, processed and will be searched for a potential match. If the match is found, an indication is shown that the prints match and successful transmission of the ID via LoRa. After transmission, the scanning device returns to the original state. The ID will be collected by the receiver module attached to the PC of the faculty, which is then accumulated in an Excel Spreadsheet using PLX-DAQ. If the match is not found, unsuccessful identification of the fingerprint is indicated.

Indications of outputs are done using different feedback LEDs connected to the Arduino microcontroller.

In PLX-DAQ, ID with time stamp is stored, along with P for present and A for absent [Figure 8]. Hence, the attendance system used in universities can not only be made automated from conventional techniques but also, an attempt is made to make it smart as well.



	A	B	C	D
1	TIME	ID		
2	12:00:00	4		
3	12:00:01	3		
4	12:00:30	5		
5	12:00:45	1		
6	12:00:56	2		
7	12:01:00	10		
8	12:01:30	12		
9	12:01:58	31		
10	12:02:00	14		

	A	B	C	D	E	F	G
1	ID	NAME	ATTENDANCE				
2	1	A	P				
3	2	B	P				
4	3	C	P				
5	4	D	P				
6	5	E	P				
7	6	F	A				
8	7	G	A				
9	8	H	A				
10	9	I	A				

Fig. 8 PLX-DAQ Entry

6.2 Results and Advantages

The transmitter device is first uploaded with the fingerprint enrolment sketch using Arduino IDE and the subject's fingerprints are recorded with second level identity confirmation with a unique ID, which is in this case, the university serial number (USN). This is the initial phase of the working of the device.

As the class is going to be held by a faculty, he/she will carry this transmission device uploaded with fingerprint verification and data transmitting sketch, to the classroom and then hands it over to the students. The students will pass on the device among themselves, after entering their fingerprints individually to the device and getting success feedback

The transmitted ID is then received by a LoRa Ra-02 receiver connected to another Arduino, which is uploaded with LoRa Receiver sketch and is connected to a personal computer belonging to the faculty which is present in the staff room.

The personal computer has PLX-DAQ running, which will detect any incoming data from Arduino. The Arduino-UNO communicates with LoRa Ra-02 using SPI Communication interface. If the sensed data is the ID of the student, then it will enter the ID to a new column of the Excel Spreadsheet along with a timestamp. If any student is absent, the spreadsheet compares it with the student database and reports present as P and absent as A in another column.

Further management of these data received like, calculation of shortage of attendance i.e. the short listing of students whose attendance is less than 85% of the total classes held.

Advantages that can be derived over conventional methods are- low power, wide range, portable, elimination of chances of fraud or proxy, increased data security, low overall cost and reduction in paperwork involved.

7. LIMITATIONS AND FUTURE WORK

(a) Slower bit rate. The transmitted data is enough for the realization of this particular application. But we cannot transmit images or huge files using the LoRa communication interface.
(b) Need for careful handling of the device.
(c) Upgrading to LoRaWAN- a MAC protocol which can connect up to 80 LoRa physical nodes like the one used here. LoRaWAN is widely used for IoT applications involving tiny sensor nodes present in remote areas. Using this technique, we can maintain the attendance of an entire department, if not an entire institution.
(d) Uploading the collected data of the attendance in the cloud or a locally hosted website for verification of the students.
(e) Mass producing this idea for implementation in different universities.

8. CONCLUSION

Automated attendance collection is achieved by using biometric (fingerprint) scanner R307 where all the registered fingerprints are stored, verified and the verified ID is sent over-the-air using LoRa™ RA-02 module. LoRa™ is a long-range and low-power telecommunication system, ideally for the "Internet of Things". The physical layer uses the LoRa™ modulation, a proprietary technology by Semtech Corporation. The sent ID is received by receiver LoRa™ module, and it is transferred to the personal computer of the faculty, ready for further processing. This paper aims to throw a light upon modern communication

protocol called LoRa™ in realizing the effective utilization of time in classrooms of universities by using it to transfer the attended students' ID on a mobile device, while the lecture is going on. The main advantage of LoRa™ is the long range of communication. Its range ideally is about 10km line of sight. LoRa™ is based on FSK modulation technique and chirp spread spectrum (CSS) which helps in elimination of echoes and Doppler Effect.

9. ACKNOWLEDGMENT

We would like to thank Dr Ambedkar Institute of Technology, India for its invaluable support.

10. REFERENCES

[1] Development of Fingerprint Biometric Attendance Management System using Wireless Connectivity, Prof. Avanti Thakkar, Bhalerao Prateek, Deshmane Rahul, International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 3.

[2] Mohammad Omar Derawi, Bian Yang and Christoph Busch, Fingerprint Recognition with Embedded Camera on Mobile phones, Norwegian information society Laboratory, Gjovik University College, Gjovik, Norway, Journal Article 2012.

[3] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones", IEEE Communications Surveys & Tutorials.

[4] Review Paper On Video Surveillance Based Attendance System Rahul V. Patil, S.B.Bangar, International Journal of Advance Engineering and Research Development Volume 4, Issue 2, February -2017.

[5] Wireless Fingerprint Attendance System Based on ZigBee Technology LI Jian-po, ZHU Xu-ning, LI Xue, ZHANG Zhi-ming Information Engineering College, Northeast Dianli University, Jilin, China

[6] A Biometric-Based Model for Monitoring and Controlling Students and Lecturers' Attendance in Tertiary Institutions, Elijah O. Omidiora, Omotayo Salawu, Stephen O. Olabiyisi, Adebisi A. Adigun, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, January 2015.

[7] Liu Ji. "The Design of Wireless Fingerprint Attendance System", 2006 International Conference on Communication Technology, November 2006.

[8] LoRa™ SX1276/77/78/79 Datasheet, Rev. 4. Semtech, 2015. Available online: http://www.semtech.com/images/datasheet/sx1276_77_78_79.pdf

[9] LoRa™ Alliance. "White Paper: A Technical Overview of Lora and Lorawan", The LoRa Alliance: San Ramon, CA, USA, 2015. [Google Scholar]

[10] IEEE 802 Working Group and Others. IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs); IEEE Std 802.15.4-2011: New York, NY, USA, 2012. [Google Scholar]

[11] Weyn, M.; Ergeerts, G.; Wante, L.; Vercauteren, C.; Hellinckx, P. Survey of the DASH7 alliance protocol for 433 MHz wireless sensor communication. Int. J. Distrib. Sens. Netw. 2013, 9, 870430. [Google Scholar]

[12] Berni, A.J.; Gregg, W.D. On the utility of chirp modulation for digital signaling. IEEE Trans. Commun. 1973, 21, 748–751. [Google Scholar]

[13] Petajajarvi, J.; Mikhaylov, K.; Roivainen, A.; Hanninen, T.; Pettissalo, M. On the coverage of lpwans: Range evaluation and channel attenuation model for lora technology. In Proceedings of the 2015 14th International Conference on ITS Telecommunications (ITST), Copenhagen, Denmark, 2–4 December 2015; pp. 55–59.

[14] LoRaWAN Specification V1.0. LoRa Alliance, 2015. Available online:https://www.lora-alliance.org/portals/0/specs/LoRaWAN%20Specification%201R0.pdf

