iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** II **Month of publication:** February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40305

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

Smart Attendance Marking System Using Bluetooth Low Energy and Facial Recognition Technology

Dr. V. Anantha Narayanan[1], S. Sriram[2], Aswin Raamanathan M[3], Nikhil Chandra[4], Varun Siddharth[5]
[1]*Amrita School of Engineering, Coimbatore, India*

Abstract: ***The process of taking attendance manually can be troublesome and time consuming. However taking attendance is mandatory in most of the educational institutions in India. The usual process of taking attendance involves the faculty manually calling out the names of the students in an order and marking his/her presence in a sheet of paper. The existing method of marking attendance is slow and students may fool the faculties in marking proxies if the classroom strength is large enough. There are various ways to automate the attendance marking process using technologies like biometric sensors , RFID cards , facial recognition , BLE beacon cards etc. This paper focuses on implementing a BLE beacon based attendance marking system with facial recognition technology for authentication. It uses BLE beacon cards communicate with android application to enable marking attendance. The app uses facial recognition technology to authenticate every user before marking attendance. This makes the process of marking attendance faster and is proxy safe.***

Index Terms: Bluetooth low energy, BLE peripheral, android, automated attendance management, facial recognition authentication, BLE encryption.

I. INTRODUCTION

The process of taking attendance manually can be troublesome and time consuming. However taking attendance is still mandatory in most of the educational institutions across the country. The usual process of taking attendance involves the faculty manually calling out the names of the students in an order and marking his/her presence in a sheet of paper. This paper is then submitted to the respective department to get recorded. The attendance rate is an important aspect in the view point of an educational institution. It is important because students are more likely to succeed in academics when they attend school consistently. It's difficult for the teacher and the class to build their skills and progress if a large number of students are frequently absent. This makes most of the educational institutions to setup a minimum attendance criteria in all subjects, every semester. This criteria has to be met by the students to clear the subjects. If not met then then the student might not be allowed to sit for the final semester exams. Implementing these strict rules regarding attendance could be a way to ensure that students attend the classes and are being evaluated on a regular basis. The conventional and manual method of marking attendance is slow and students may fool the faculties into marking proxies if the classroom strength is large enough. This paves way to create a system that helps in marking attendance faster and proxy safe.

One of the popular method of marking attendance in the industry is by using a bio metric scanner system [11]. When a person keeps his finger in the scanner the scanner recognizes the thumb impression and the attendance of the person is directly updated to the database. But in the case of educational institutions such universities and colleges attendance is marked in an hourly basis,having all the students of a class use one or a few biometric sensor to mark attendance is more time consuming than the conventional method [1]. Other methods like a bar-code scanner or an RFID scanner also possess the same disadvantage.

The solution presented in this paper is a fast and proxy safe attendance marking system using state of the art technologies like Bluetooth Low Energy sensors, facial recognition tech- nology etc. These sensors come in a card form with other necessary peripherals naming BLE cards, which can then be given as an ID card to each recipient. Each card advertises a unique string which is used to identify each card uniquely. These cards are then coupled with an android application which is used to mark attendance by the students and monitor by the faculty. This application is set to sense all the BLE cards in the range of 5m.The range of the sensing can be set up to 40m depending on the size of the room this system is intended to be setup. When the faculty wants to collect attendance he/she opens the android application and collects data from all the BLE beacon cards present in the proximity.

In the meantime the students open their android app to mark attendance. In this way the attendance can be marked in a faster way. Each student is able to mark attendance only if these following conditions are met.

First the students have to be authenticated by a face recognition authenticator [2]. After authenticated they can only mark attendance only if their BLE card is present in proximity. The BLE card data must be read by both the faculty and students app during the time of attendance. This makes sure that both the student and the faculty must be within the range of 5m from the card while taking attendance.

These conditions make sure that the right student is in the class during the time of attendance, thus avoiding proxies. The data received is then pushed to a database where the final attendance list is computed and stored. This makes the students to track their attendance faster , rather than waiting for it to be updated in a weekly or a monthly basis.

This system allows various visualization of the attendance data for useful insights. It also allows the faculty to make manual changes in the attendance list in the need of manual mitigation. This system can also be adopted to various other scenarios where attendance is recorded frequently to a large group of people.

II. BLUETOOTH LOW ENERGY

Bluetooth Low Energy (BLE) is a low power wireless technology used for connecting devices with each other. BLE operates in the 2.4 GHz ISM band, and is targeted towards applications that need to consume less power and may need to run on batteries for longer periods of time—months, and even years. This is the right technology for this application because the beacon cards transmit less data and is needed to last in a battery for a longer duration of time. Most of the operating system including android supports Bluetooth low energy.

There are two modes in which Bluetooth low energy works. They are the broadcasting mode and communication mode. The broadcasting mode is a one way communication mode where the data is advertised repeatedly to be received by all the receivers.

Communication mode is a two way communication mode where the BLE peripheral first advertises itself. The client if wishes establishes a connection with the peripheral to enable two way exchange of data. Once connection has been established between the client and the peripheral all the data exchanged id encrypted with a tight industry standard 128- bit AES data encryption [5]. When pairing of the client and peripheral occurs a temporary key known prior to both the client and peripheral is used to generate a long term key which is then used to encrypt the communication.

For this application we have built a custom BLE peripheral using nRF52 development kit by Nordic semiconductors. The nrf52 DK is a versatile single board development kit for Bluetooth Low Energy, Bluetooth mesh, NFC, ANT and 2.4 ghz proprietary development on the nrf52810 and nrf52832 socs. It can be powered by USB, but also includes a CR2032 battery holder, enabling in-field testing of prototypes [12].The life of the battery depends on the application that runs but , the battery typically lasts for more than a year.

The custom BLE peripheral developed broadcasts the fol- lowing services:

1) Ble admin service
2) Battery service
3) Device information service.

III. FACIAL RECOGNITION AUTHENTICATATOR

Facial recognition is a bio-metric technology that is used to recognize people by distinguishing facial features to identify a person . The major advantage of facial recognition is its safety and security. Facial recognition systems importance is increasing day by day. A lot of work has been done in the area. Due to the more advancements in the field of convolution neural network facial recognition has become more accurate and accessible. Facial recognition system provides a quick secure and automatic verification experience [9][2]. We use face recognition algorithms to authenticate a student. In this way a student has to be using the phone for marking the attendance. He can't handover his smartphone and his BLE card to another person to mark attendance for him. For this we will be fine-tuning a renown facial recognition algorithm called facenet and implement it in our system.

A. Dataset Used

The final data set created contains over 1800 images belonging to 10 classes. Initially 20 images of each class was captured from various angles orientation and varying background .These conditions are a must for a robust training of the CNN [6]. The original dataset of 200 images is then augmented using various noise and brightness conditions to make the size of the dataset from 200 to 1800

B. Face Detection

Multi task cascaded neural network is used to detect and align the faces. MTCNN network is made up of 3 individual neural network which are the p-net , r-net and o-net. The p- net creates pyramids of the same images with different sizes. A 12*12 kernel runs through each image for identifying faces making up 3 convolutional layers . Then 2 probabilities, namely presence or absence of face is calculated in the 4th convolution layer. R–net takes the inputs from the P –net and calculate more accurate bounding boxes. O –net takes inputs from R – net and calculates the probability of face detected, box coordinates and facial features like eyes coordinates as explained in [3].The facial areas detected using this algorithm is then used for further processing

C. Data Augmentation

Data augmentation is an important step to improve the performance of the proposed system. It is used to increase the number of samples and diversity in the dataset [2]. The detected images using the MTCNN are then augmented using different noise and brightness conditions. The face detected images are added with Gauss noise and Impulse noise in- dividually. The 200 images are then made into 200 images with no noise, 200 images with Gaussian noise and 200 images with impulse noise making the total images count to 600 images. Then the 600 images are added to a brightness of -25% (darken), 0% (original) and +25% (brightens). Thus the 600 images are converted to 1800 images of 10 classes respectively.

Fig. 1. Dataset sample images

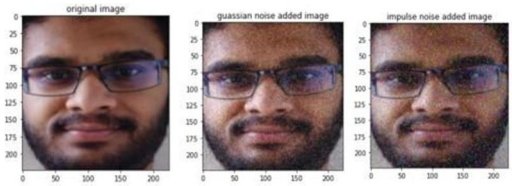


Fig. 2. noise added images

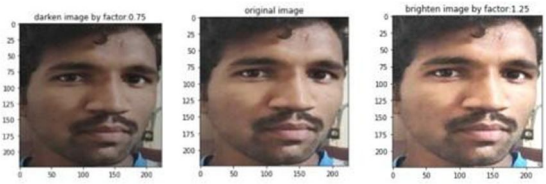


Fig. 3. brigtness added images

D. Face Recognition

This system uses a pre trained CNN for face classification. A typical CNN architecture consist of an input layer, convolution layer, pooling layer, fully connected layer and a output layer. There are different activation functions, softmax functions, loss functions involved as well [6].

The input layer provides the images to the convolution layer specifying the size of the image including height width and channel size. The convolution layer does the feature extraction using 2d convolutions using several filters. The pooling layer decreases the size of the feature maps and reduces reluctant information. The fully connected layer identifies patterns using the features learned using the layers mentioned before. The softmax layer is used to provide classification probabilities to the classification layer , which is then used for assigning inputs to the one of many mutually exclusive classes.

We have used FaceNet for facial feature extraction and SVM for classification. FaceNet is a face recognition system developed in 2015 by researchers at Google that achieved then state-of-the art results on a range of face recognition benchmark datasets as explained in [6]. The FaceNet system can be used broadly thanks to multiple third-party open source implementations of the model and the availability of pre- trained models. facenet achieves 99.63% of accuracy in the LFW dataset having standard deviation of + or - 0.09 as explained in [9][7]. We use a pretrained FaceNet Inception

ResNet v1 keras model provided by Hiroki Taniai[10]. This model is trained on MS-celeb-1M dataset. The model is then modified such that the number of predicting classes is set as 10. The input images has to be coloured and to have an input shape of 160 *160 pixels in RGB channel. The model outputs a 128 element vector knows as face embedding's corresponding to each input image. The face embedding's are then normalized and are fitted into a Support Vector Machine(SVM).We use linear kernel in SVM. The SVM model is trained and used for prediction.

Fig. 4. predictions from facenet

E. Experimental Results

This section presents the results obtained during the experimentation. This experiment is was carried out using colab notebooks with 12GB RAM in a 2VCPU xenon processors at 2.3GHz and a 100gb free space. The deep neural network models were trained using a Tesla k80 with 12GB of RAM and with a compute if 3.7.

The augmented dataset containing of 1800 images of 10 subjects were divided into 80% for training and 20% for testing. The facenet inception resnet v1 shows an accuracy of 98.3%.

The classification report of the testing set can be seen in table 1.In face verification the precision of the model is very important than recall. Because a correct person can be recognized wrong and again he can try to verify his face . But a incorrect person should not be verified as a correct person . Facenet has a good precision(0.986) and accuracy(0.983).The confusion matrix produced is seen in table 2.

Name	Precision	Recall	F1-score	Support
Aswin M	1.00	1.00	1.00	36
Akash	1.00	0.83	0.91	36
Aswin S	1.00	1.00	1.00	36
Bharath	1.00	1.00	1.00	36
Krishna	0.86	1.00	0.92	36
Nikhil	1.00	1.00	1.00	36
Rishab	1.00	1.00	1.00	36
Sriram	1.00	1.00	1.00	36
Varun	1.00	1.00	1.00	36
vasanth	1.00	1.00	1.00	36

Table I
Classification Report for Facenet on Testing Set

IV. CLONING SAFE BLE CARD:

A beacon is a simple device that constantly emits a radio signal. Further more, all communication with a beacon hap- pens "in the clear" and isn't encrypted. As beacons are rapidly becoming gateways to complicated interactions that have a financial motivation, there's increasing incentive for someone to use your beacons in ways you hadn't intended. There is a possibility that the BLE card that is provided to a student may be cloned by passive eavesdropping by a hacker. If the BLE card provided to a student is cloned then the student use the cloned BLE card to make his presence be in 2 or more places at the same time. This voids the very architecture of our system. To solve this issue should implicate an encryption algorithm to the BLE card so that only authenticated users may only know the data that the BLE card is transmitting so that no unauthorized person can eves drop the data. We plan to implement a AES ECB based encryption to the BLE card to preserve its novelty.

Name	Aswin M	Akash	Aswin S	Bharath	Krishna	Nikhil	Rishab	Sriram	Varun	vasanth
Aswin M	36	0	0	0	0	0	0	0	0	0
Akash	0	30	0	0	6	0	0	0	0	0
Aswin S	0	0	36	0	0	0	0	0	0	0
Bharath	0	0	0	36	0	0	0	0	0	0
Krishna	0	0	0	0	36	0	0	0	0	0
Nikhil	0	0	0	0	0	36	0	0	0	0
Rishab	0	0	0	0	0	0	36	0	0	0
Sriram	0	0	0	0	0	0	0	36	0	0
Varun	0	0	0	0	0	0	0	0	36	0
vasanth	0	0	0	0	0	0	0	0	0	36

Table II. Confusion Matrix for Facenet on Testing Set

Electronic code book is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plain text and output is in form of blocks of encrypted cipher text. the proof of work of AES based encryption is discussed in [5]. Generally, if a message is larger than b bits in size, it can be broken down into bunch of blocks and the procedure is repeated. ECB is a block cipher; the result of the encryption depends solely on the contents of the input buffer and the key. The consequence of this is that encrypting two buffers that have identical contents will always yield identical results. As the BLE card advertises the same data over and over again , this algorithm mentioned above cannot be directly applied for a solution .

We have modified the algorithm in such a way that it best fits the system. The firmware and the app both possess a pre shared unique 128 bit key. When the app finds the presence of our custom BLE peripheral it tries to connect with it automatically. The firmware uses the random number generator peripheral to generate a unique 128 bit NONCE before advertising. The firmware makes this NONCE readable via an authentication characteristic in the BLE admin service for the app to read. Once the app has read the nonce both the firmware and the app encrypts the nonce using a 128-bit AES ECB cypher to create a challenge response. The phone writes the challenge back to the firmware using the RX characteristic.

The firmware receives the challenge response and then authenticates it. If the authentication is successful then the firmware allows the app to let read the admin characteristic in the BLE admin service through which the app can know the novelty of the card. If the authentication is incorrect then the firmware disconnects with the app preventing it from reading the other characteristics.

For the next connection the firmware generated another unique nonce This prevents an unauthorized device to connect with the ble card to know the protected characteristics which is used to assure the novelty of the BLE card.In this way we can be sure that only the authenticated app can perform communication with the custom BLE peripheral.

VI. ANDROID APPLICATION

A. Application

The application is divided into two separate android app intended to two types of users namely, the faculty and student. The app contains two parts JAVA AND XML. All the layouts and user interfaces are done in the XML part, where core logic and functionality of that activity is written in the java part.

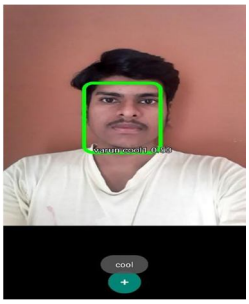


Fig. 5. facial recognition based authentication

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

The student and the faculty app has a login facility where the user is intended to login. The credentials are assumed to be provided prior by the administration body. The username and password entered by the body is then matched with the data in the database. If the credentials are matched then the user can proceed further else the user is prompted with the message “incorrect credentials” and is allowed to try again.

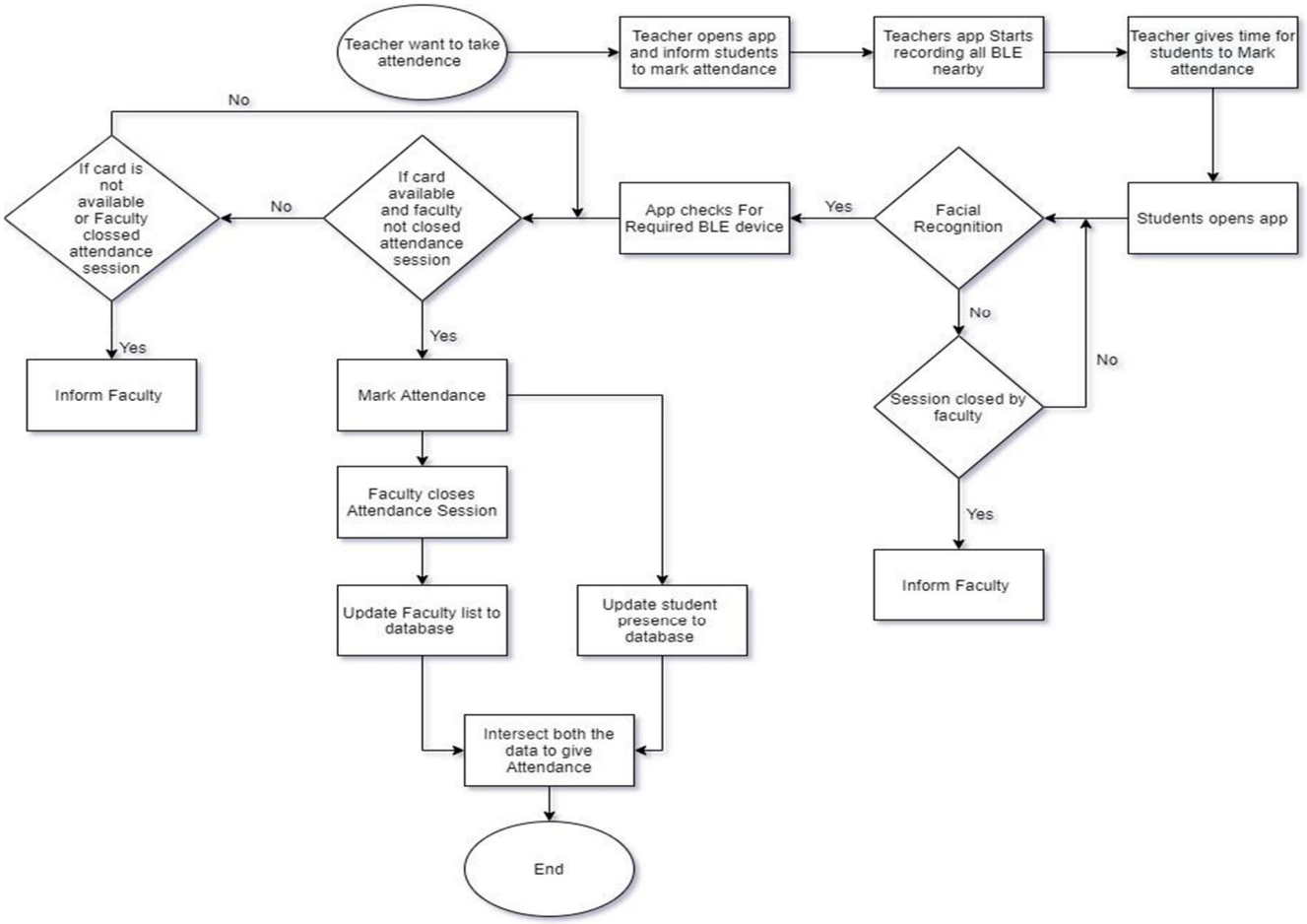


Fig. 6. Flow diagram of the system

In the students app after login the student is prompted with the facial recognition authenticator. This is to make sure that the right student is using the app to mark attendance. The facial recognition authenticator is implemented in the application with the help of frameworks and predefined libraries like MediaPipe, Android LibSVM and Tensorflow. once a person shows his face to the camera , the app tracks the face of the person and recognizes him. The name of the classification and confidence level displayed in the overlay view for reference as seen in figure 5.

Once the student face has been verified, he moves to the marking attendance activity. The student clicks the mark attendance button to record his attendance in the database. The app then checks for the customized BLE peripheral card of that particular student to be in proximity. If BLE card is in proximity, the attendance is successfully recorded in the database . If the customized BLE card is not in proximity then student prompted with a “not in proximity” message. The student will be allowed to try again until the faculty closes the attendance session.

In the faculty app after login the faculty gets to choose the class he wants to take attendance for. Once the class has been selected he moves to a page where he can start taking attendance. The faculty starts taking attendance by clicking the start attendance button. This then starts the activity where the UUIDs of all the custom BLE peripherals in range is captured as seen in figure 7. When the faculty ends the attendance these data are pushed into the database for the generation of the final attendance list. After the attendance session if any issue is found in the attendance, the faculty can take manual actions to resolve the issue. The faculty can add students to the list or remove.

B. Measures to Avoid Proxy

Avoiding proxy is an important part in the field of marking attendance. It is a major huddle that has to crossed to make sure that students attend classes regularly and grow their skillsets. The whole architecture of our proposed system revolves around to avoid proxies. We have adopted certain methodologies and conditions in our system so that students cant mark proxies.

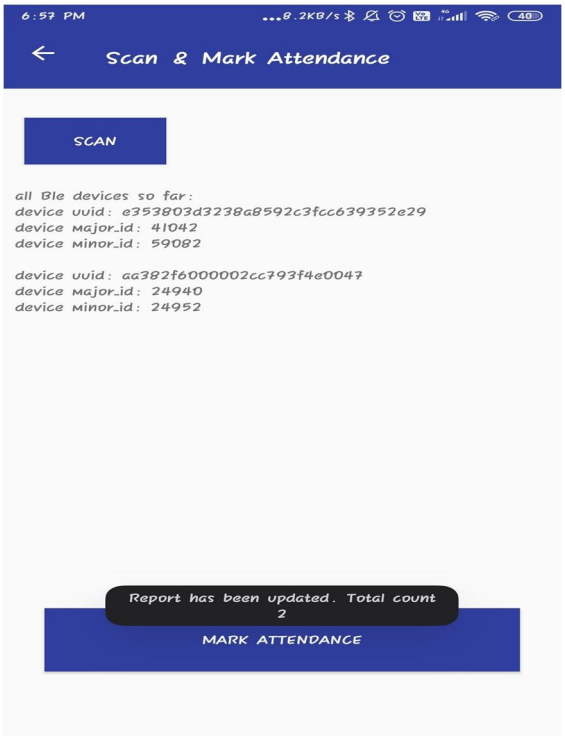


Fig. 7. Capture of nearby BLE card details

The app lets a person to mark attendance if and only if his BLE card is in proximity. That BLE card data is been captured by both the student and faculty while marking attendance. This prevents a person from being elsewhere and marking attendance.

The app does not allow any other user to mark attendance for another person even if he has the BLE card of the other. We have implemented a facial recognition authenticator that authenticates the user right before he or she marks attendance. Another way to void this architecture is by cloning the BLE card. A student can then make the presence of his BLE card be in the classroom and with him at the same time and mark attendance from elsewhere. To avoid this possibility we have made our own custom BLE peripheral card, which can't be cloned because of its data encryption strategy. The combination of the following conditions and methodologies will make marking proxies tough.

VII. PROCESS

Each student is given an individual custom BLE card that broadcasts and admin service and can be identified by unique UUID, major and minor id. This unique string is then identified by the android application that the students and the faculty in the class to mark attendance. When it is time to mark attendance in the class the faculty starts the attendance session. The students uses his smart phone to authorize himself using face recognition authenticator. Once the app confirms the presence of the student then he is allowed to click a button to mark attendance. This button is only active when the application senses the student's particular BLE card to be present in range. When the student clicks the button his presence is recorded in the database. In the meantime the faculty's phone picks up the unique string present in all the BLE cards in range. The range of BLE beacon card is limited to 5 meters. The range can be modified based on the size of the room. Once the faculty closes the attendance session, the list of unique string collected by the faculty's mobile is also then pushed into the database. This then calls a cloud function that compares the list from both the students and faculties' side and the intersecting list of students is finally given attendance. The final attendance list is then stored in the database. In this way the attendance is taken in less than a minute. The detailed flow of the system can be seen in figure 6. This system can also be adapted to various other scenarios where attendance is recorded frequently for a large group of people.

VIII. CONCLUSION

Taking attendance is mandatory in most of the educational institutions in India. The usual process of taking attendance involves the faculty manually calling out the names of the students in an order and marking his/her presence in a sheet of paper. This reported is then submitted by the faculties to the respective department in a weekly or a monthly basis.

The traditional method of marking attendance is slow and students may fool the faculties in marking proxies if the classroom strength is large.

We were able to develop a system that makes the process of marking attendance easy, fast and proxy safe. This system saves lot of manual labour effort and time.

We used technologies like BLE , Facial recognition using tensor flow , an-droid studio to make it happen.

We were able to implement various face recognition algorithm choose the beat and implement it in the project.

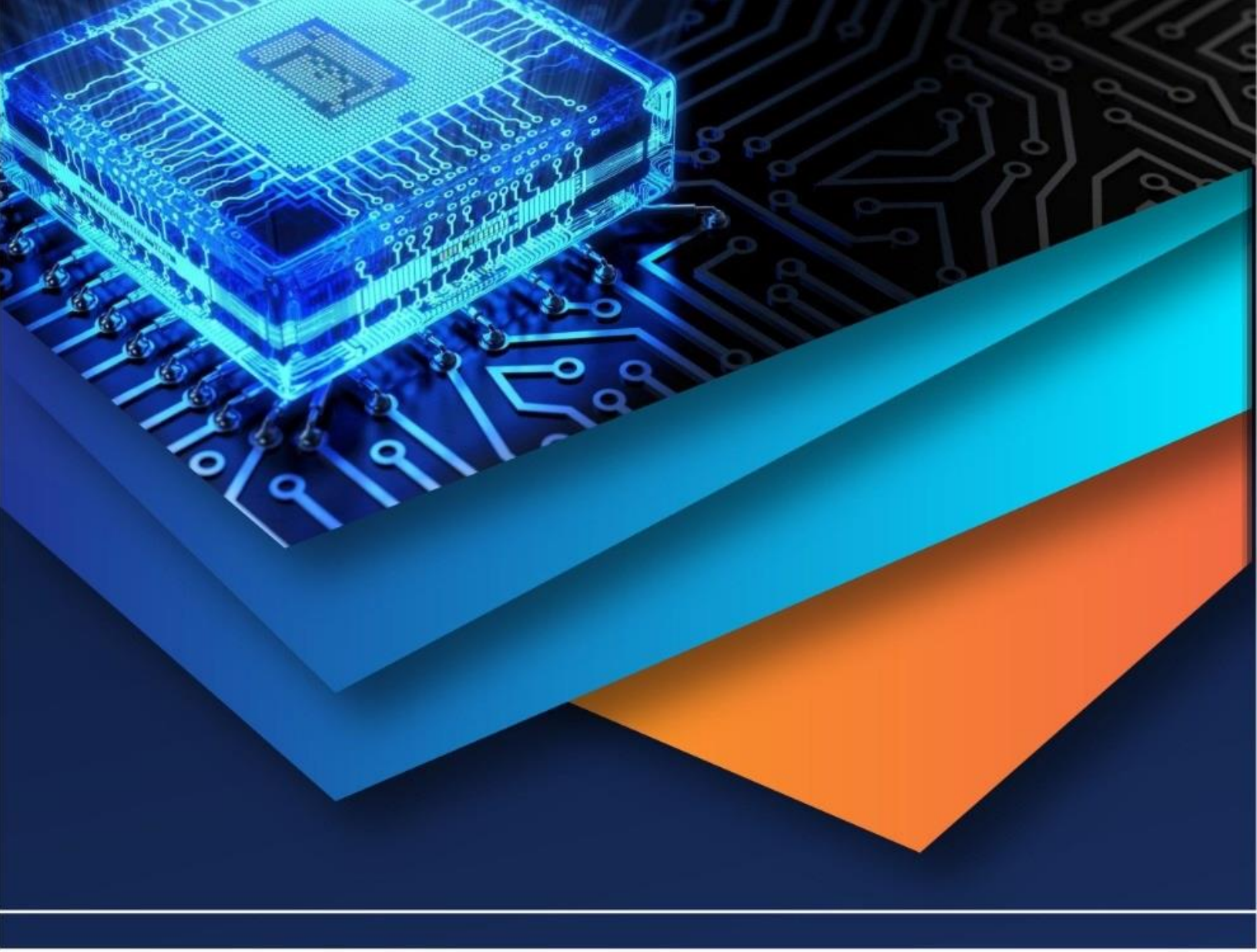
We were able to encrypt the BLE beacon card communication to prevent unauthorized users from eves dropping the data emitted by the card. This prevented the card from being cloned. In the future we intend to make this application far too reachable by implementing it on all major operating systems like IOS , windows etc.

We may include BLE beacon receivers all over the campus and implement a tracking feature for easier access to the student inside the campus.

We intend to increase the capacity of the database and the server to accommodate lot of new users.

REFERENCES

[1] Raghav Apoorv and Puja Mathur Smart Attendance Management using Bluetooth Low Energy and Android , 2016 IEEE Region 10 Conference (TENCON)
[2] Maheen Zulfiqar , Fatima Syed , Muhammad Jaleed Khan , Khurram Khurshid Deep Face Recognition for Biometric Authentication , Proc. of the 1st International Conference on Electrical, Communication and Computer Engineering (ICECCE) 24-25 July 2019, Swat, Pakistan
[3] Kaipeng Zhang, Zhanpeng Zhang, Zhifeng Li, Senior Member, IEEE, and Yu Qiao, Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks , Senior Member, IEEE
[4] Sode Pallavi, V Anantha Narayanan An Overview of Practical Attacks on BLE Based IOT Devices and Their Security, Amrita School of Engineering, Coimbatore, India 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS)
[5] Khoongming Khoo, Eugene Lee, Thomas Peyrin and Siang Meng Sim, Human-readable Proof of the Related-Key Security of AES-128
[6] Masaki Nakada, Han Wang, Demetri Terzopoulos , AcFR: Active Face Recognition Using Convolutional Neural Networks , University of California, Los Angeles
[7] O. M. Parkhi, A. Vedaldi, A. Zisserman Deep Face Recognition British Machine Vision Conference, 2015
[8] FaceNet: A Unified Embedding for Face Recognition and Clustering by Florian Schroff, Dmitry Kalenichenko, James Philbin arXiv:1503.03832 [cs.CV]
[9] Deep Face Recognition: A Survey ,Mei Wang, Weihong Deng 2018,arXiv:1804.06655
[10] Facenet github link https://github.com/nyoki-mtl/keras-facenet
[11] Biometric Attendance System:Engr. Imran Anwar Ujan and Dr. Im-dad Ali Ismaili Institute of Information Communication Technology, University ofSindh, Jamshoro, Sindh, Pakistan Proceedings of the 2011 IEEE/ICME International Conference on Complex Medical Engineering May 22 - 25, Harbin, China
[12] Nrf52 DK nordic [online]: https://www.nordicsemi.com/Software-and- Tools/Development-Kits/nRF52-DK
[13] K. Nimmy and Dr. M. Sethumadhavan, “Biometric Authentication via Facial Recognition”, 2014. Amrita School of Engineering, Coimbatore, India



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY