Wireless Connectivity to Vehicle Body Control Module

Rutuja Uday Biraj
Dept. of Electronics Engineering
Walchand College of Engineering, Sangli

Dr. Amrita A. Agashe
Dept. of Electronics Engineering
Walchand College of Engineering, Sangli

Abstract:- The project aims to build an application in the area of internet of things, wireless technology and automotive electronics. It also aims to locking and unlocking of two wheelers using wireless technology and then sharing the vehicle using smart phone. The basic idea is to provide access to only authorized people for sharing a two wheeler vehicle securely. Authorization for the same can be done via sharing necessary credentials. A customized Android based application is devised. It should be installed on the smart phone. This is linked up to embedded controller based digital lock and unlock via Bluetooth interface.

The vehicle needs to have a Bluetooth based body control module (BCM). Whenever a person wants to operate vehicle using smart phone he must be within that Bluetooth range of BCM. The range of Bluetooth is nothing but the received signal strength by the device in that area. After matching with the credentials and received signal strength indicator (RSSI) value, the vehicle is unlocked. The concerned vehicle status with time and date is recorded in the application platform and is updated on the cloud using GSM technology. To check for the proposed system and its results, prototype is implemented. Successful operation is confirmed after its experiments with different approaches.

***Keywords*:-** *IoT, Embedded System, Wireless Communication, Processor and Controller, Android, Bluetooth Technology, Automotive Electronics.*

I. INTRODUCTION

The use of mobile devices has been exponentially increasing nowadays. No doubt they are meant for convenience of human beings. Along with the basic functions of dialing a number, texting a message or easing with mobile banking they have been performing functions for controlling our daily lives as well. Smart phones and its mobile applications help us control numerous devices like TVs, projectors, air conditioners and so the cars.[1]

Normally people use general locks with keys. However, it’s a fear of losing keys. A solution for this has been proposed in our paper. This proposed system aims to remotely lock/unlock vehicles using wireless communication technology. The Bluetooth embedded smart phones provide remote locking for the vehicles as it can be handily managed.

This includes integrating smart phone, its mobile application, the controller and an array of sensors. The task goes in realizing a smart vehicle based lock-unlock system and allowing it to smoothly share among the authorized persons. The authorized people can access this information globally via smart phones.

II. RELATED WORK AND TECHNOLOGIES

The proposed remote vehicle lock system relates to the technologies as follows:

Presently the locks are categorized into three types: the key lock system, the password lock system, and the remote lock system. Of these, the key lock is the oldest one. Many people fear to lose the key which makes them to carry along with. The password lock has an advantage over this but a disadvantage of people forgetting passwords. To overcome these issues a previously made patent paper, was built up on Bluetooth technology. It followed three basic steps: first one contains transmitting an address that we want to control from a mobile terminal to a Bluetooth device. The corresponding Bluetooth device registers the received address as the unlocked address.

Second step works according to external keys and is in search of Bluetooth device in the list and checks whether the above terminal is registered or not. Then selecting a Bluetooth device from user it transmits the address wirelessly. Third step includes judging the address transmitted by the device and then initiating the lock/unlock activity accordingly. But this system has some flaws. The Bluetooth information can be hacked by a non-authorized person and in turn vehicle can be unlocked. Second flaw includes a user losing his/her password leading to unlocking difficulty.

Many of the discussed problems are taken into account to build the objectives of our proposed system For ex. the need to carry a key is resolved by using mobile device itself which acts like a key.

Second, since the application of user itself provides a way to easily manage it’s passwords thus the problem of forgetting passwords is resolved. Third, even when the user forgets a password, there is step by step procedure for user to open the lock. The following figure 1 also shows how remote lock system is to be designed.

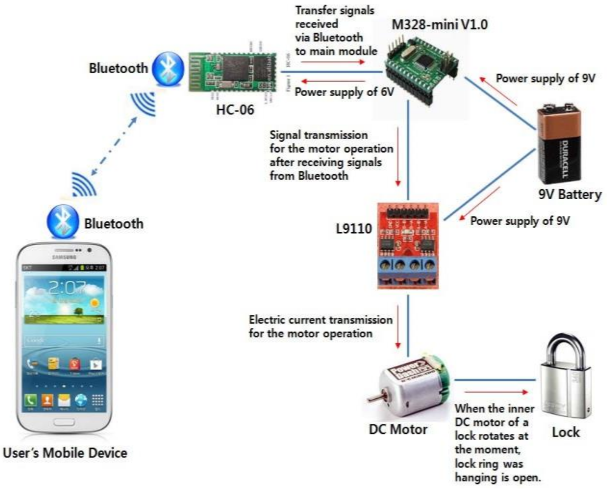

Transfer signals received via Bluetooth to main module
M328-mini V1.0
Bluetooth
HC-06
Power supply of 6V
Power supply of 9V
Signal transmission for the motor operation after receiving signals from Bluetooth
9V Battery
Bluetooth
L9110
Power supply of 9V
Electric current transmission for the motor operation
DC Motor
When the inner DC motor of a lock rotates at the moment, lock ring was hanging is open.
Lock
User's Mobile Device

Fig 1:- System architecture for the remote lock system

➢ *Android*

Android is an open source software and a mobile operating system. It is a modified version of Linux based kernel. Moreover it acts as middleware, User Interface (UI), browser and application as well. It has C/C++ libraries as the components of Android system. [2]

The system architecture for Android Open Source based on stack numbered up to 6 piles, viz. Applications, Android Framework, Native Libraries, Android Runtime, HAL/HIDL, and Linux Kernel. [3]

➢ *Bluetooth*

Bluetooth technology nowadays is embedded in mouse, keyboards, industrial automation and home automation devices along with smart phones. It can catch up to seven nearby devices at a time. The area in the range of device is being called Pico net. Pico net frequency can controlled by master device. Data is transmitted frame by frame. There are two different links of master/slave devices in the network: the Asynchronous Connection-Less (ACL) link and the Synchronous Connection-Oriented (SCO) link. The first link comes into picture when data is to be collected for processing. ACL link is the only link that connects a slave unit to a master unit. SCL link is important for sending real time data.[4]

For establishing a Bluetooth connection, the device name and address is must. Now select the destination Bluetooth address where the data needs to be transmitted. Put on a pairing request sharing password. Repeat till devices are totally paired. Accept the connection when pairing is completed. Figure. 2 shows Bluetooth connection procedure.

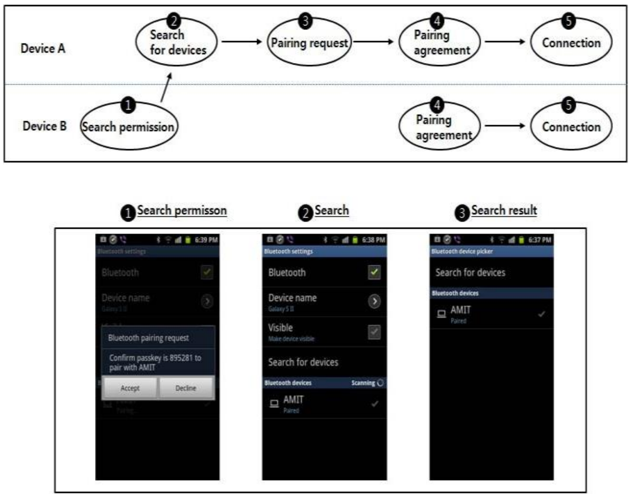


Fig 2:- Bluetooth connection procedure.

Bluetooth Security Manager is one of the security services in-built in this technology. This service works on the three principles viz. authentication, confidentiality, and authorization. The legal rights for Bluetooth devices are controlled at the link level. Figure 3 tells us the configuration of Bluetooth security manager. Logical Link Control and Adaptation Protocol (L2CAP) in the Bluetooth protocol stack looks after communication over the host ACL link. It receives requests for connection. Then the security manager checks the access. It finds service database and the device database if exists and then it applies proper authentication or encryption. If the security manager grants the access to the L2CAP then connection is setup. [5]

The characteristic features of the security manager include 1. Information of security management related to services 2. Information of security management related to devices 3. Questions and answers related to security of protocol along with application safety.

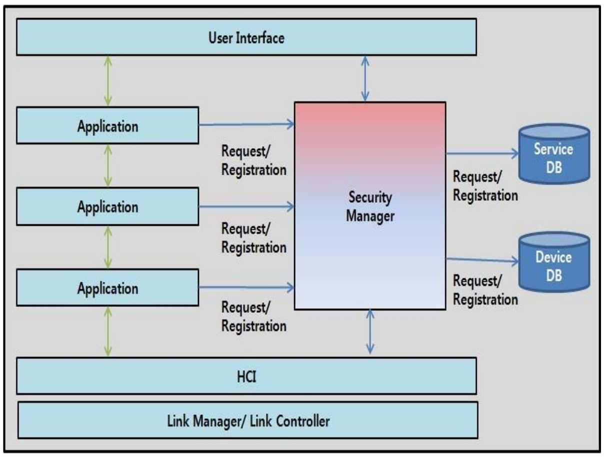


Fig 3:- Configuration of the Bluetooth security manager.

III. THE PROPOSED SYSTEM ARCHITECTURE

The proposed system over here is being implemented in two wheeler vehicle. Two wheeler vehicles contain body control module which serves the purpose of controlling and diagnosing all electronics parts included in the vehicles. The system gives a wireless control to vehicle body control module. That means controller is being interfaced with Bluetooth low energy module and GSM module. A dedicated android application installed on users' mobile phone controls this vehicle access system. This vehicle will be able to share with multiple users securely. Figure 4 shows the system block level diagram.[9]

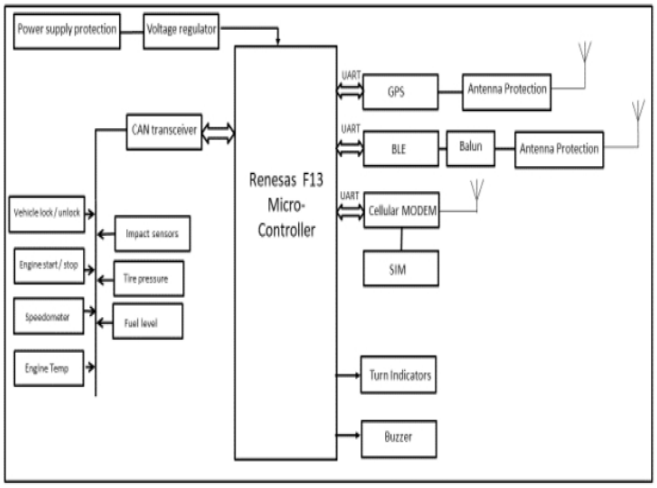


Fig 4:- The implemented system block level diagram.

Here the controlling action has been though Renesas F13 auto qualified microcontroller which will act as body control module. The system has cellular connection through Bluetooth low energy chip and GPS/GSM chip. Both have their respective antennas for range. The communication to Bluetooth Low Energy (BLE) and GSM/GPS from controller is through UART protocol. This communication is serial one. The transmitting UART device need to change from parallel (controlling unit as CPU) to serial at the receiving end of UART. Then this receiving UART converts back to parallel for receiving unit. Data transmission and reception is from Tx and Rx pins of UART.

Controller Area Network (CAN) bus is a standard protocol for effective communication. CAN transceiver is interfaced with numerous sensors which will receive the status of vehicle. These include engine temperature, tire pressure, vehicle speed, acceleration etc. It initiates communication between devices and controller without host computer. This protocol is designed mainly to reduce wiring harness in the vehicles. Devices transmit data frame by frame sequentially. This is upon the priorities, high priority one's continue the communication when low priority one interrupts. This also gives prior indications of locking unlocking provided by turn indicators and buzzers. All devices are supplied with voltage regulators for smooth, steady and regulated power supply.

IV. METHODOLOGY

The prototype of above said system is implemented. The functions for the same are described one by one in following sub-sections.

- *Authentication:*

Users for the vehicle are categorized into two:

1. Default (primary) user
2. Secondary users

Users can be shuffled into one another using settings mode of android application. For the first time access, manufacturer provides the password. Then this user becomes a default user. The default user can reset the system password upon using reset password function in android application. Default user log-in remains active, no need to log-in again.

- *Vehicle Access:*

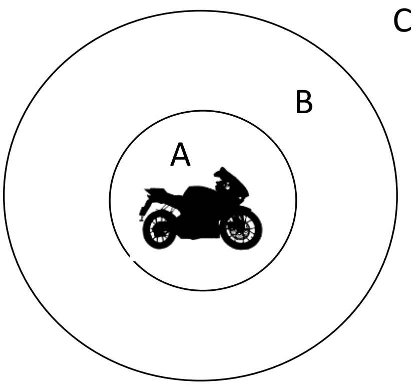


Fig 5:- Area is divided around the vehicle

The BLE range counters over the vehicle's vicinity as shown in figure 5. Once the authorized user crosses outer boundary and enters in region B, Bluetooth connection is set-up in system and in users' android application. The user is identified with his previously entered credentials. Now the cloud takes over the vehicle access status via GSM technology. Vehicle gets unlocked after the user crosses inner boundary.[8]

The change in received RSSI value by the system pre-decides the threshold. Now the unlocked status is shown by the blowing horn once and blinking indicators for 1 sec. This activates most of the functions of vehicle like engine, low beam etc.

When the user crosses the outer boundary and enters in region C, Bluetooth connection is set-down. The vehicle gets locked once the connection is lost. Even when the vehicle is moved out of region A the vehicle gets locked. This status is shown by blowing the horn once and blinking indicators for 2 sec each. The mobile application keeps sending the RSSI value to the system at regular intervals as long as the user is in the regions A and B.

- *Vehicle Sharing:*

Vehicle can be securely shared by the default user using share vehicle option in the application. Mobile number and password of the intended user needs to be entered by the default user. The corresponding password is sent to intended user's mobile number to give him the access to the vehicle. This intended user must be in the shared users list of default user. Now both the mobile number and password are sent to the system via GSM. The intended user must install dedicated android application to access the vehicle.[9]

Once the intended user enters in region B then he should enter previously shared password in mobile application. After entering the password, the system verifies first the mobile number then checks whether the password matches the password sent by default user. After this login proceeds successfully, the intended user can share the vehicle.

V. FLOWCHART

The flowchart for the proposed system is shown in figure 6. The flowchart is executed every time when a vehicle access request is originated by one of the users, let it be a default user or an intended one. It has loops for processing important steps as of connecting BLE, accessing a vehicle by user, checking user for crossing inner boundary or outer boundary.

The user should enable his Bluetooth in the mobile phone. Once the user enters in the region B, the application in his mobile gets connected to the vehicle. The user should enter his credentials as password only one time and next time he is paired by default. Now the system checks for cellular connectivity. If connection is established then login activity is updated in the cloud. The system lock/unlock functions are now being executed. The manual lock/unlock functions is provided by default. According to user's position and RSSI value, the vehicle is locked or unlocked. The indications as discussed above for locking and unlocking vehicle with respect to horn and indicators are executed accordingly.

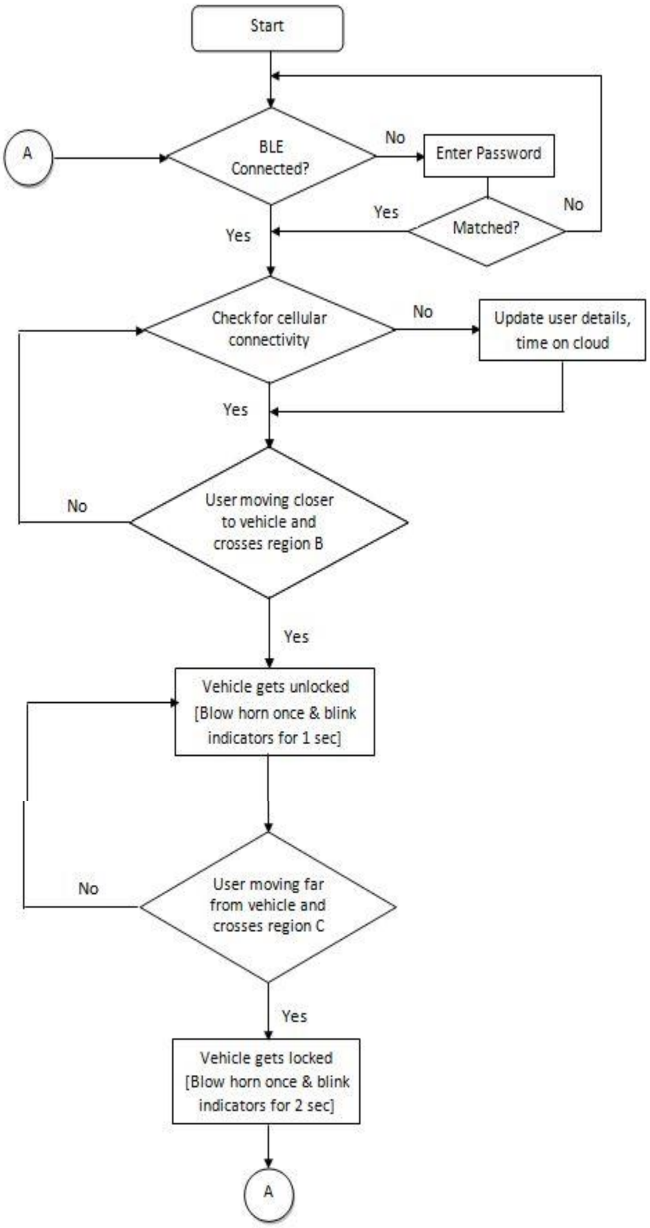

Start
A
BLE Connected?
No
Enter Password
Yes
Matched?
No
Yes
Check for cellular connectivity
No
Update user details, time on cloud
Yes
No
User moving closer to vehicle and crosses region B
Yes
Vehicle gets unlocked [Blow horn once & blink indicators for 1 sec]
No
User moving far from vehicle and crosses region C
Yes
Vehicle gets locked [Blow horn once & blink indicators for 2 sec]
A

Fig 6:- Flowchart for proposed system

VI. RESULTS

A smart lock/unlock system using Bluetooth, GSM/GPRS as communication technology is implemented. This is being tested with the prototype and discussed in this paper. The utility for sharing vehicle is also discussed.

The application is being developed in JAVA software platform. This application is built page wise. The commands to be executed by the controller are being sent by Bluetooth interface. The starting page of this application is shown in figure 7. Different components are integrated to these pages at the time of developing.[6]

Fig 7:- The opening page of the application.

Cloud gets updated by the status of the system at regular intervals. The credentials stored are verified for authentication purpose. The authorized users can access this data any time and everywhere.

The commands are given by the user randomly. Those are being sent wirelessly via Bluetooth from mobile phone to the controller. Now these commands are executed by the controller with the help of developed application configured on Renesas F13 microcontroller. To open the application, manufacturer provides the password for the first time. Henceforth, user can reset the password or keep the same and proceed further.[7] Reset password page of the application is shown on Figure 8.

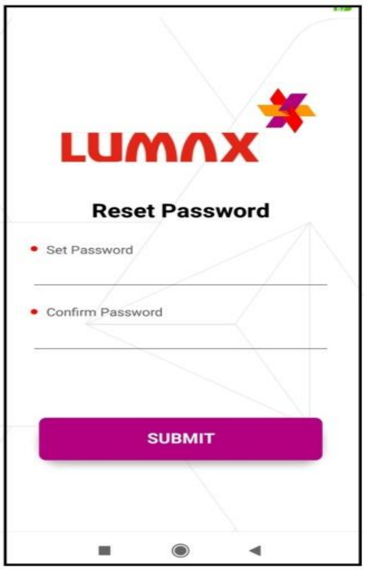
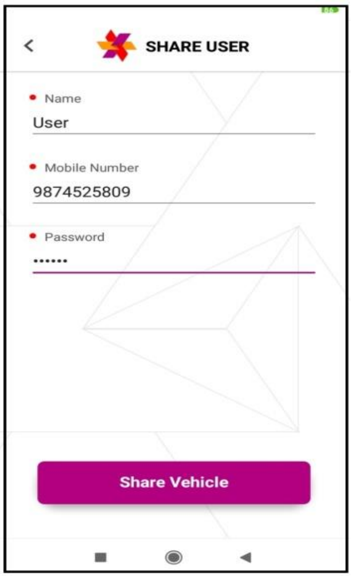


Fig 8:- Reset password function in the application.

Now if the user wishes to share his vehicle then the intended user's name, mobile number must be entered by him first. After successful login attempts of the intended user, his name is added in shared vehicle list of default user's application. He can use the vehicle as long as he is authorized by the default user. The default user can add, remove the entries in the shared vehicle list. The share vehicle function page in the application is showed in following figure 9.



Name
User

Mobile Number
9874525809

Password
••••••

Fig 9:- Share vehicle function in the application.

The experiments are performed on the prototype to check functions. The prototype is shown on Figure 10.

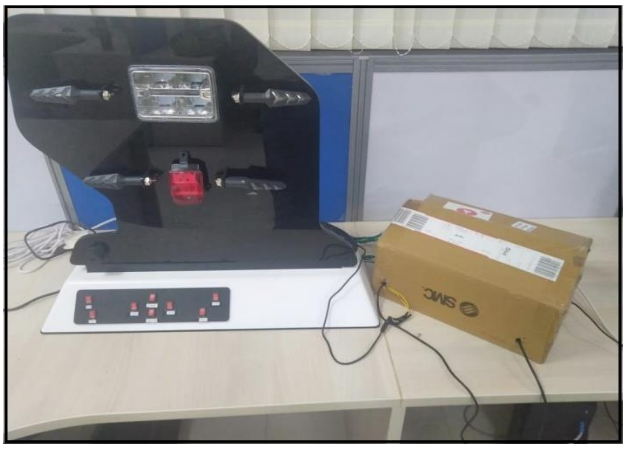


Fig 10:- The prototype of the proposed system

VII. CONCLUSION

This paper gives a brief discussion on smart vehicle lock unlock system based on Bluetooth and GSM/GPRS. Cloud technology is smartly being used. Android based smart phone application is integrated with Bluetooth and controller.
.

The proposed system successfully operates within the range of the Bluetooth. The system prototype is user friendly. Anyone with a little knowledge of vehicle electronics can easily match with it and operate. The system is quite interactive and the application bit innovative. There’s a lot more scope for students in building new concepts. Once you get triggered with the basics you are almost done.

The security parameters are taken into consideration a bit more. This is to safe-gourd the vehicle while sharing with unknown user as well. Wireless approach takes over the wiring harness, which is quite complicated in the vehicles.

The future scope includes taking this over to four wheeler vehicles. This will add a lot more sensors, its integration and taking all over to the cloud for monitoring the status. More over parameters of cars such as tracking, remote engine break, petrol consumption, CO2 emission speed, etc also is added to give us the track of vehicle for efficiency.

REFERENCES

[1]. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, L , “Internet of things for smart cities”, *IEEE Internet of Things journal, 1(1), 22-32. (2014).*

[2]. Wei, J., “How Wearables connect with the Cloud and the Internet of Things: Considerations for the developers of wearables”, *IEEE Consumer Electronics Magazine, 3(3), 53-56. (2014).*

[3]. Spanò, E., Niccolini, L., Di Pascoli, S., & Iannacconeluca, G., “Last-meter smart grid embedded in an Internet-of-Things platform”, *IEEE Transactions on smart grid, 6(1), 468-476. (2015).*

[4]. Jeong, Hae Duck J., Jiyoung Lim, Wooseok Hyun and Woojin Lee., “A Remote Lock System Using Bluetooth Communication”, *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2014*

[5]. P Bhagwat, “Bluetooth : Technology for short-range wireless apps”, *IEEE Internet Computing, vol 5 2001*

[6]. J. Sanchez, S. Dormido, R. Pastor and F. Morilla, “A java/Matlab-based environment for remote control system laboratories: Illustrated with an inverted pendulum”, *IEEE Transactions on Education, vol 47, 2004*

[7]. X. Li, W. Shu, M. Li, H.-Y. Huang, P.-E. Luo, and M.-Y. Wu, “Performance evaluation of Vehicle-based mobile sensor networks for traffic monitoring”, *IEEE Transactions on Vehicle Technology, May 2009*

[8]. A. R. Al-Ali, I. Zualkernan and F. Aloul, “A mobile GPRS-sensors array for air pollution monitoring”, *IEEE Sensors J October 2010*

[9]. N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista and M. Zorzi, “The deployment of a smart monitoring system using wireless sensors and actuator networks”, *IEEE Smart Grid Comm. 2010.*

[10]. Agrawal, D. P., & Zeng, Q. A., “ Introduction to wireless and mobile systems”. *Cengage learning 2015*

[11]. Farrand, W. A., Flatten, O. H., & Walter, H. (1963). U.S. Patent No. 3,105,927. Washington, DC: U.S. Patent and Trademark Office.

[12]. AppInventor, M. (2015). MIT App Inventor. Technical report, http://appinventor. mit. edu/explore.