IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Automatic Portal Lock Security Using Two-Step Verification via Bluetooth and GSM

Sherin Abraham[1], Ashwin Achari[1], Vishwadeep Shinde[1], Akash Shinde[1]

Indira College of Engineering and Management, Maval, Pune[1]

Abstract: IoT has emerged as a new concept for smart- security oriented system. IoT is basically connecting embedded devices to internet. IoT includes embedded devices along with software, sensors, actuators and network connectivity to collect and exchange data across the network. IoT has become an integral part in security domain. Bluetooth technology from mobile combined with real time monitoring system can be used for security and automation. Instead of using traditional locking system (ex. key-lock), Bluetooth can be used as an alternative. Bluetooth can be used for securing portals like doors, lockers, etc. but Bluetooth can be spoofed. To overcome this, two way authentication can be introduced where first step will be Bluetooth pairing, second will be answering a predefined question via Morse code interface and also using an authenticator generating time based code. This will reduce the chance of Bluetooth spoofing and provide better security in the field of IoT.

Keywords: Door Locking System, Sensor, GSM, Bluetooth, Embedded System.

I. INTRODUCTION

Internet of Things (IoT) is the interconnection of the uniquely identifiable embedded computing devices within the existing internet infrastructure. So IoT is basically connecting embedded system to internet. IoT consists of a network of physical devices, vehicles, buildings and other items embedded with electronics, software's, sensors, actuators and network connectivity that enable these objects to collect and exchange data. The concept of IoT first became popular in 1999, through the Auto-ID center at MIT and related market-analysis publications. With the emergence of IoT, smart cities have come into picture, making remarkable advancement in technology and automation-controlled human life. With this, security also needs to be taken care of providing reliability in all aspects.To improve security, an IoT device that needs to be directly accessible over the internet, should be segmented into its own network and have access restricted. Action should be taken if there is anomalous access into the system.

II. SYSTEM ARCHITECTURE

The System Architecture is divided into 3 modes:
1.Mode1: Frequent Access
2.Mode2: Password based Access
3. GSM: Remote Access

Mode 1: Frequent Access
This mode consists of a simple step wherein recognized user (owner) connects to microcontroller fitted onto the portal via his mobile's Bluetooth and access is granted depending on whether the user's Bluetooth address is present in microcontroller's list of recognised Bluetooth addresses or not. The purpose of this mode is for frequent access of the portal, where user is in vicinity of the portal and wants to access it on the regular basis. But if the user is going far away from the vicinity of the portal then it is recommended that the system should be kept in mode 2 as in mode 1, Bluetooth address if spoofed then without recognised user in the vicinity of the portal unrecognised user can access the portal with the spoofed address.

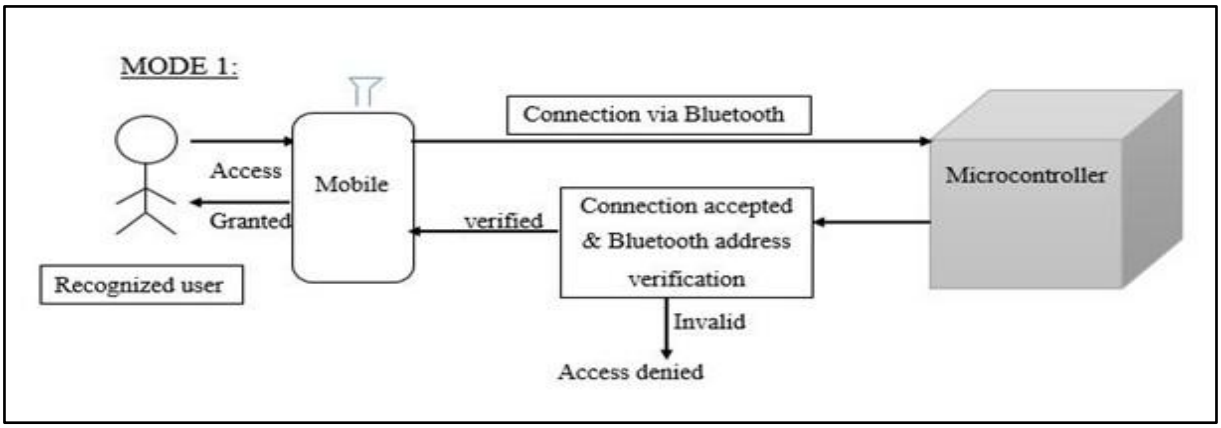

Fig1: System Architecture for Mode 1

DOI10.17148/IJARCCE.2017.63147

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Mode 2: Password based Access

This mode is for password secured access of the portal for enhancing the security of the system. Bydefault the user first enters into mode 2. After accessing the portal, a timer starts during which the system will be in mode 1. After few minutes, when the timer stops, the system will switch back to mode 2. This is to help the recognised user to frequently access the system when he is in the portal's vicinity and also to prevent any other user to access the door if recognised user has gone away from the portal and has forgotten to set the system to mode 2.

In this mode, mode 1 procedure is followedi.e. mobile's Bluetooth connection establishment with microcontroller's Bluetooth and checking of connected Bluetooth address in the microcontroller's recognised list. Then the user is supposed to enter password via Morse code interface from his mobile. (Suppose his password stored in microcontroller is 88, Morse code will be ---.. ---..). There will be an authenticator application running in user's mobile as well as in the microcontroller. This application will generate a time based password (ex. At time 1 p.m., authenticator code will be 234).

The authenticator's code will mergewith the Morse code password in the mobile and then will be sent to microcontroller (ex. 234 & 88 = 23488). An authenticator present at microcontroller will also generate same code as of user's device (ex. 234 at 1 pm). Microcontroller checks for the input received from the mobile & if it matches with code generated by its own authenticator & the password stored in it then user will be granted access to the portal.

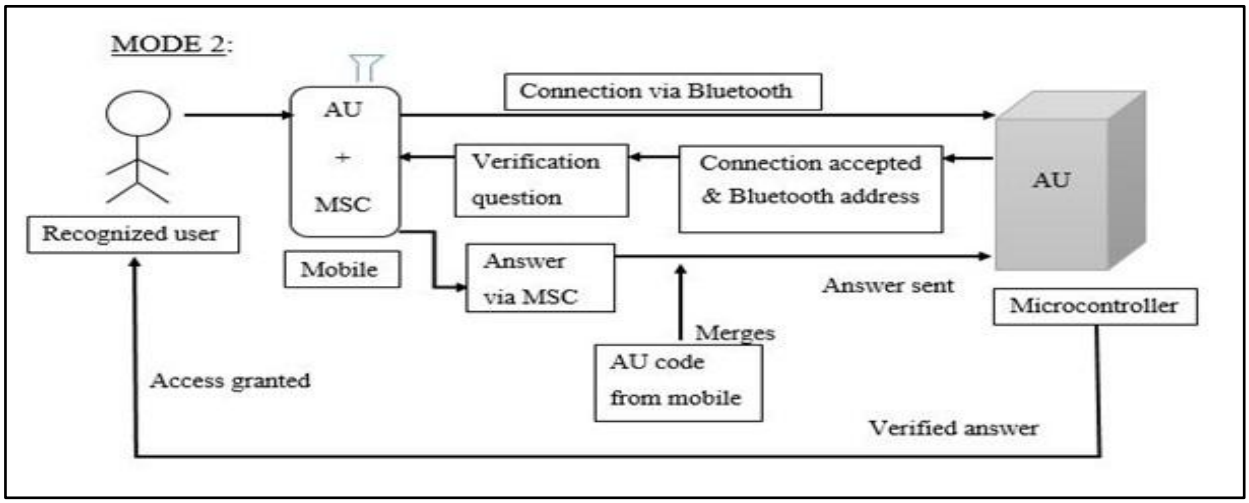

Fig 2: System Architecture for Mode 2

GSM: Remote Access

This mode is for remote access of the system. Recognised user can open the portal remotely using DTMF module attached with the system. Remote access becomes necessary for getting access to the portal in case of any emergency like loss of mobile (which is the primary media to access the portal) of recognised user or if the recognised user want to gie access to any third person who is not registered with the system and the recognised user is away from the system.

Remote monitoring can also be achieved as sensor and camera will keep track of activities occurring near portal. Sensor will sense human presence and send signal to microcontroller, it will then activate camera. Camera will then capture snapshots and it will be mailed to the user.

In this system, recognised user calls the DTMF's mobile. The call will be auto received and user will dial password from his/her mobile through the call. This password will be sent to DTMF decoder and converted internally. If the password matches then user will be granted access remotely.

III. COMPONENTS AND TECHNIQUES USED

Components and Techniques used for execution of all the 3 modes i.e. mode 1, mode 2 and GSM.

- User's Bluetooth: It is used as the media for accessing the portal. User's Bluetooth address should be registered along with password in the microcontroller's list for granting access to the portal.

- HC-05 Module: It is a Bluetooth module that will be attached with microcontroller. User will connect its Bluetooth with this module.

- Sensors: It will sense human presence and send camera activation signal to microcontroller.

- Camera: It will capture images and send it to microcontroller, where it will be mailed to the user.

- DTMF Decoder: DTMF or Dual Tone Multi-Frequency Decoder will be used for remote access of the portal.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

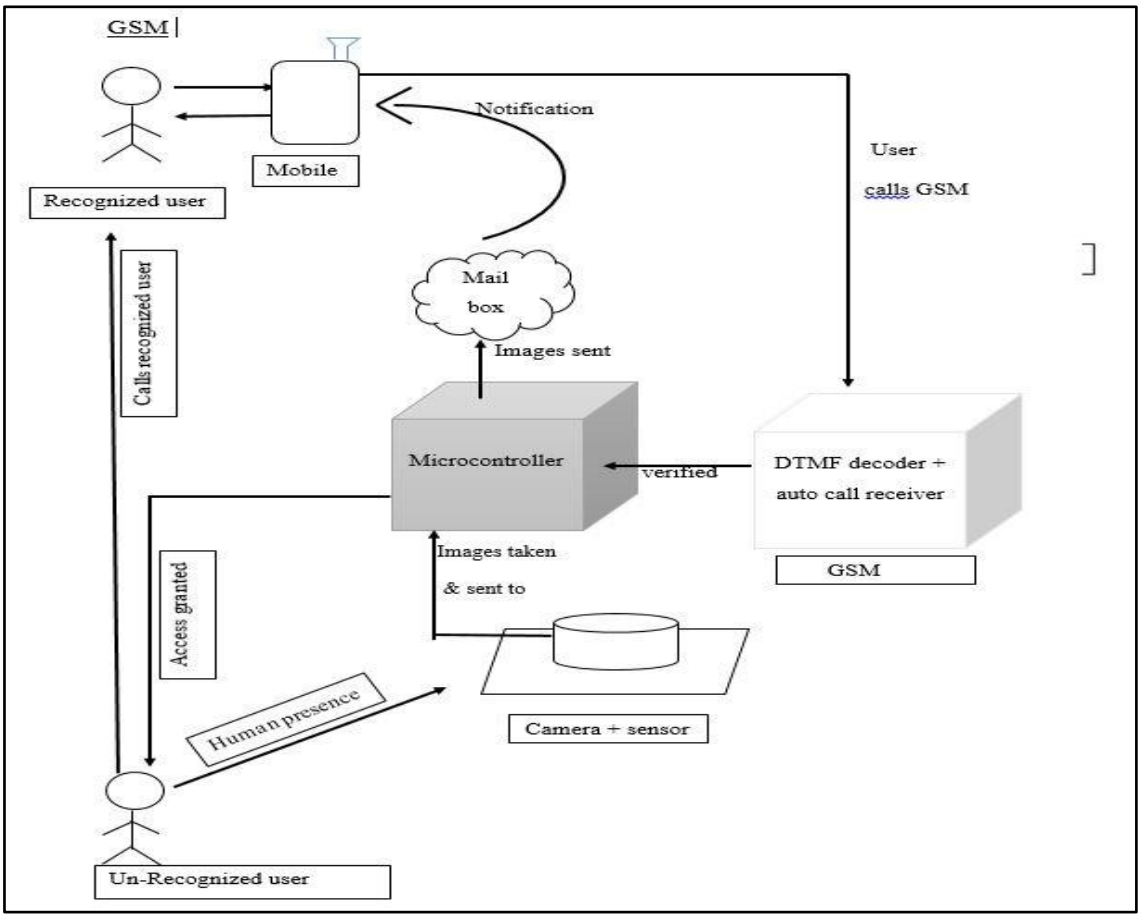

Figure 3: System Architecture for GSM

• Authenticator code: It is a one-time code that will be generated in both user's mobile and microcontroller. Same code will be generated in microcontroller as that in user's mobile depending on which registered Bluetooth address is connected to it. This code makes the mobile- device specific i.e. code will be different for different registered users even at same period of time for same portal. (ex. User 1 code will be 123 at 2 pm and for User 2 code will be 826 at same 2 pm depending on which recognised address is connected). This will not allow other users to spoof address and gain access due to different authenticator code generated in their mobile (if they have the app installed.)

Morse code Interface: It is an interface which will be replaced instead of regular interface to enterpassword for privacy. User must enter answer in dot (.) and dash (-) format in Morse code. The screen can also be kept blank for more privacy. Then instead of typing dot (.) and dash (-), user can tap the screen to give dot (.) and long press the screen to give dash (-). This will prevent others from knowing your password.

IV. ALGORITHM

1. Start
2. Initialize system ← Mode 2, Timer, tm_start ← 0, tm_stop ← 5 minutes
3. HC-05 waiting for connection
4. Connection established
5. Mode 1:
6. If (Portal accessed requested &&timer != tm_stop)
7. if (system ← mode 1)
8. check Bluetooth address
9. if (Bluetooth address ← not registered)
10. Deny Access
11. else
12. Grant access and ask to set system to mode 2
13. if (system mode ← not set)
14. system ← mode 1
15. set timer ← tm_start
16. Goto Step 5
17. else if (system mode ← set)
18. system ← mode 2
19. Goto step 23
20. Else if (timer = tm_stop)
21. system ← mode 2
22. Goto step 23
23. Mode 2 :
24. if (Portal accessed requested&& system ← mode 2)
25. check Bluetooth address
26. if (Bluetooth address ← not registered)
27. Deny Access
28. else
29. Wait for password entry

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

30. if (password ← correct && authenticator code ← matches)
31. Grant access and ask to set system to mode 2
32. if (system mode ← not set)
33. system ← mode 1
34. set timer ← tm_start
35. Goto Step 5
36. if (system mode ← set)
37. system ← mode 2
38. Goto step 23
39. Stop

V. CONCLUSION

Lock security via Bluetooth with two way verification, with remote access to your system and also providing privacy with Morse code technology along with authenticator provides more security to the portals. Hence this technology can be used not only in home doors but also in lockers, cabins, offices, server rooms, etc. making it reliable. Its advantages are keyless entry, enhanced security, regular notification on human presence and remote access. The disadvantages are Bluetooth connectivity problem, network connection and moderate code provision in Morse code.

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the project report on ' Automatic Portal Lock Security Using Two StepVerification via Bluetooth and GSM'.
We would like to take this opportunity to thank Almighty God for being with us and giving us the knowledge and understanding to make this project. We are grateful to Principal **Dr. Sunil Ingole** and Vice Principal and HoD **Dr. Poornashankar** for their indispensable support and suggestions. We would like to thank our internal guide **Prof. Sinu Nambiar** for giving us all the help and guidance we needed. We are really grateful for her kind support. Her valuable suggestions were very helpful. In the end our special thanks to our parents for giving us the moral support and encouragement for our project.

REFERENCES

[1] DhirajSunehra"ImplementationofInteractiveHomeAutomationSystemBasedonEmailandBluetoothTechnologies"Dept.ofElectronicsandCommunicationEngineering,2015
[2] DhirajSunehra,"AnIntelligenceSurveillancewithCloudStorageforHomeSecurity"Dept.ofElectronicsandCommunicationEngineering,2014
[3] SarthakJain,AnantVaibhav,"RaspberryPiBasedInteractiveHomeAutomationSystemthroughEmail"Dept.ofElectricalandElectronicsEngineering,2014
[4] N.H.Ismail,ZarinaTukiran,N.N.Shamsuddin,"AndroidBasedHomeDoorLockApplicationviaBluetoothforDisabledPeople"FacultyofElectricalandElectronicsEngineering,2014
[5] AdnanIbrahim,AfhalParavath,AswinP.K.,ShijinMohammedIqbaland ShaeezUsmanAbdulla,"GSMBasedDigitalDoorLockSecuritySystem,"Dept.ofAppliedElectronicsandInstrumentation,2015
[6] Hae-Duck,J.Jeong,JiyoungLimandWooSeokHyun,"ARemoteLockSystemusingBluetooth Communication"Dept.ofComputerSoftware,2014
[8] JoshPottsandSomsakSukittanon,"ExploitingBluetoothonAndroidMobile Devicesfor Home Security Applications" Dept. of engineering, 2015
[9] s S.Rajadurai,P.P.Nehru,R.Selvarasu,"AndroidBasedHomeSecurity andDeviceControlusingGSM"Dept.ofEIE,2015