ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

A Novel Design for Prevention of Vehicle Theft using IoT

Anshika Agarwal[1], Deepali Virmani[2]

U.G. Student, Department of Computer Science, Bhagwan Parshuram Institute of Technology, Delhi, India[1]

H.O.D (IT), Department of Information Technology, Bhagwan Parshuram Institute of Technology, Delhi, India [2]

ABSTRACT: The security of a vehicle due to the possibility of theft has always been a threat to its owners as it is one of the expensive assets that a person can own. In this paper, a system is proposed to provide greater safety in order to reduce the probability of vehicle theft. It introduces a smart anti-theft system for vehicles based on the concept of Internet of Things. It deals with controlling the vehicle's ignition remotely via mobile phone through online text messaging. The intention behind the system design is to provide communication between the owner and the vehicle so as to give him a remote access to control his/her vehicle's engine function. The proposed system is smart enough to detect the trusted owners. Every time the system senses an ignition, it makes an attempt to authenticate the owner. In case authentication fails, the system immediately turns off the engine and prevents the vehicle from being stolen. Besides ignition controls, it captures the image of the intruder and emails it to the owner for the records after uploading it to the cloud.

KEYWORDS: Engine control, Internet of Things (IoT), Raspberry PI 3, SMS (Short Messaging System), Vehicle Anti-Theft System.

I. INTRODUCTION

Security concerns are increasing every day, in every field of living, be it vehicles, homes or the family members. Focusing on the vehicles, this paper proposes a system, called as SVATS i.e. Smart Vehicle Anti-Theft System which can provide freedom from the concern of your vehicle getting stolen when parked. This system is based on the technology of Internet of Things i.e. IoT, due to its wide use in the development of new products.

A report in Times of India [1] read that a vehicle is being stolen every 13 minutes in Delhi, India. [2] states that in 2014, the average interval between car thefts was 23.6 minutes which was reduced to 13 minutes in 2015. One fifth of all IPC crimes in Delhi are of vehicles and these seem to be getting organized better by the day. High-end vehicles with built-in security systems aren't much safe before the professionalism of these skilled car boosters. Most security features in cars today like central locking, steering handle lock, anti-theft alarm system seems efficient but increasing crime rates are an indicator of the inefficiency of such technology.

The intention behind the system design is to provide communication between the owner and the vehicle so as to give him a remote access to control his/her vehicle's engine function. The proposed system is smart enough to authenticate its owner once it senses an ignition. In case authentication fails, the system immediately turns off the engine and prevents the vehicle from being stolen.

The following could be possible scenarios of vehicle access:

- Scenario 1 (When the user accesses his vehicle)

In the situation where the owner himself or someone in the knowledge of the owner accesses the vehicle, the moment an alert SMS i.e. Short Messaging System is sent to the owner, he may reply with the password message to turn off the system and not affect the working of the engine.

- Scenario 2 (When the intruder accesses the vehicle)

In the case where an intruder tries to steal the vehicle, the owner may once turn off the engine deliberately by responding to the alert SMS with any message. This turns off the engine. If the user hasn't replied to the alert message

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

in a stipulated time period, an alert call is made to user's cell phone. Failure to respond to the alerts in due time triggers a security threat and the system shuts the engine off automatically.

After the engine getting shut down once, if the intruder tries to restart the engine, the system would automatically turn it off again, smartly detecting an unauthorized access. Hence the vehicle doesn't get very far from the parking place.

II. NEED FOR IOT BASED VEHICLE ANTI-THEFT SYSTEM

In [3-11] many systems have been proposed. These have their limitations. Some of these limitations are listed below:

1. The system in [3] is visible to everybody and can be damaged by the thief.
2. In [4,5], the system is restricted to Android platform in mobile phones which would make it impossible to authenticate the user from another type of mobiles.
3. The system in [7] works on door locks and hence is not implementable on two-wheelers.
4. In both [6,9], the hardware used is neither cost effective nor efficient.

Thus, based on the requirements of today's world, this paper presents an anti-theft system which overcomes these limitations to provide the following features to its users:

1. It is not visible to the third person and hence cannot be damaged or tampered with.
2. Its usage is not restricted to mobiles with Android platform.
3. It can be implemented on all type of vehicles (with engine).
4. It provides a remote access of engine control to the user.
5. It is very cost effective and efficient.
6. Since it senses the ignition, the car doesn't get to go far from the parking space and can be easily located.
7. It takes care of the worst-case scenario i.e. when the user is unable to respond to theft alerts timely and shuts off the engine automatically.
8. Since the functioning time of the system is short in comparison to those working for as long as the vehicle is running, it does not heat up enough to pose any working issue.

III. EXISTING SYSTEMS

Besides these proposed systems, there are existing systems which have certain limitations over the proposed system presented in this paper. Table 1 compares the features of existing systems with those of the proposed SVATS System.

TABLE I. FEATURES OF EXISTING SYSTEMS COMPARED TO HSDL SYSTEM

Name	Features					
	Smart	*Camera*	*Alarm*	*Alert Notification*	*Visibility*	*Cost*
Bike Disc Lock by Vheelocityin [11]	×	×	✓	×	✓	Low
TK06 by TRAK [12]	✓	×	✓	✓	×	High
Airbag Steering Wheel Lock [13]	✓	×	✓	×	✓	Very High

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Name	Features					
	Smart	*Camera*	*Alarm*	*Alert Notification*	*Visibility*	*Cost*
Wheel Lock Clamp [14]	×	×	×	×	✓	Medium
Clutch Lock by Qunhu [15]	×	×	×	×	✓	Medium
IP Cam Wifi Anti Theft [16]	✓	✓	✓	×	×	High
SVATS System	✓	✓	✓	✓	×	Medium

In Table 1, the comparison among various features of some of the best existing systems like Bike Disc Lock by Vheelocityin, Clutch Lock by Qunhu etc. has been made with the proposed system i.e. Smart Vehicle Anti-Theft System. Thus, from this comparison, it can be easily concluded that the proposed SVATS System is better than some of the best existing systems especially in terms of security and alarming features. It is a hybrid combination of all the features that are missing from current existing systems.

IV. PROPOSED SYSTEM DESIGN

1. System Prototype

Fig.1 gives the overall project outline in terms of hardware connections. Raspberry PI 3(PI) is the heart of the proposed system. With this, the motor, the vibration sensor, the camera and the alarm are attached. As the battery turns "ON" it allows PI to connect to the available internet and activate its functionality. Once it receives signals of ignition, it sends an online alert as an SMS to the owner. Similarly, it makes an alert call and uses the internet to mail the captured image of the intruder to the owner. Thus, the system takes inputs from the vibration sensor, camera, and motor, the processing is done by PI and output is given by camera, motor, and alarm.

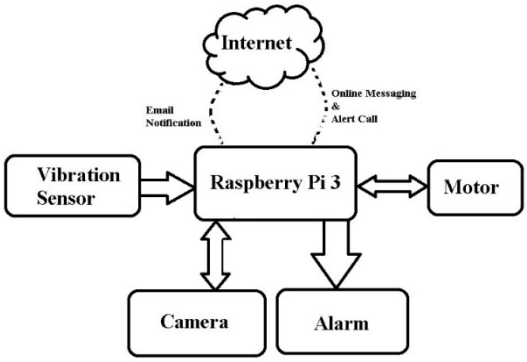


Figure 1. System prototype of proposed system

Fig.1 as mentioned above, gives the structural layout of the system. It shows the various hardware components connected together, to communicate over cloud, and provide security to vehicles. The internet cloud is used to provide notifications and receive commands to and from the owner of the vehicle regarding the authenticity of the person accessing the vehicle. Thus, it shows the input output connections of various hardware with the main component i.e. PI.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

2. System Flow Analysis

Fig. 2 gives a flow analysis describing step by step working of the proposed system.

The system starts whenever PI connects to the internet. Whenever the ignition is detected for the first time, the user is alerted via a notification message. The system then waits for a message from the user for a stipulated time. The moment a response from the user is received, an attempt to user's authentication is made. After successful user verification, the message is mapped with a preloaded password.

If password match is a success, then access to the vehicle is authorized and the system shuts itself down. But if the user authentication fails or the message received is not the password, the system shuts the engine OFF.

Also, if the owner fails to reply in given time, an alert call is made, and the system waits for user's response. Any further delay by the user triggers a security threat and the system shuts the engine OFF automatically.

Now, if the intruder tries to ignite the engine again after being forced to shut down for the first time, the system is smart to sense it and turns off the engine again without having to repeatedly notify the owner or wait for further authentication.

Hence, theft is controlled as shutting down of engine recurrently provides enough delay to alert the authorities and stop the vehicle from getting stolen.

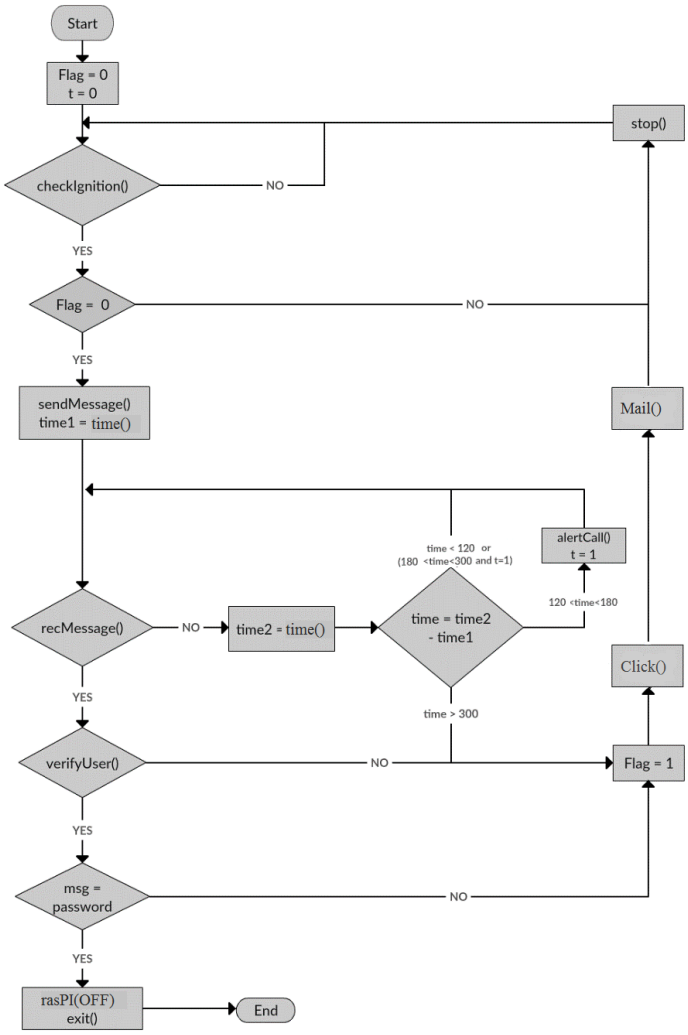


Figure 2. Flow Analysis of the proposed system

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Thus, Fig.2 gives the pictorial representation of working flow of the proposed system. It lists down the point of use of various functions like checkIgnition(), sendMessage(), Mail() etc. The definition of all such functions are given in detail in the next section.

V. SYSTEM ALGORITHM

1. Checking the ignition

checkIgnition ()
1. if (piezo = HIGH) and if (flag = 0)
2. sendMessage()
3. return true
4. else return false

2. Send an Alert Message

sendMessage()
1. msg = "Alert!! Possible Intrusion!!"
2. client.messages.create(to="+918476429128", from_="+16173509121",body=msg)

3. Check message from the owner

recMessage (msg)
1. if (Message.available())
2. if (verifyUser() = true)
3. if(msg=”#superman!”)
4. return 1
5. else return 2
6. else return 0

4. Click the photograph

Click()
1. camera= PiCamera()
2. camera.start_preview()
3. time.sleep(1)
4. camera.capture('/home/Driver.jpg')
5. camera.stop_preview()

5. Making an alert call

alertCall ()
1. call = client.create(to="+918447920158", from_="+16173908121”)

6. Verification of the owner

verifyUser ()
1. if (sender_chat_id == 12345623)
2. return true
3. else return false

7. Shutting down the engine

stop ()
1. GPIO.output(27,False)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

8. Send an email

```
Mail()
1. msg0['Subject'] = str("Intruder in vehicle")
2. msg0['From'] = 'system@abc.com'
3. msg0.attach(MIME("Hi, please find the attached image"))
4. part1=open("/home/Driver.jpg").read()
5. msg0.attach(part1)
6. server= smtplib.SMTP("smtp.gmail.com")
7. server.login("system@abc.com", "abc")
8. server.sendmail(msg0['From'],recipients,msg0.as_string())
```

9. Vehicle Anti-theft system

```
main ()
1. flag=0, msg='', t=0
2. abc: ignition = checkIgnition ()
3. if (ignition = true)
4. time1 = time.now ()
5. else goto abc
6. xyz: var = recMessage(msg)
7. if(var=0)
8. time2 = time.now ()
9. time=time2-time1
10. if (time< 120|| (120< time < 300&& t=1))
11. goto xyz;
12. else if (120<=time<=180 && t=0)
13. alertCall ()
14. t=1
15. goto xyz;
16. else flag = 1
17. else if (var=1)
18. system(OFF)
19. exit(0)
20. else flag = 1
21. if (flag = 1)
22. Click()
23. Mail()
24. stop()
```

VI. RESULT

The results in Fig 3 to 7 were obtained when the system was made to perform all of the functionalities depending upon the responses to the alert notification from the owner.

1. Basic System Functionalities

Basic system functionalities are those which the system performs irrespective or the fact that whether the user authentication was successful or not. The following figures i.e. Fig. 3-5, represent the various basic functionalities of the proposed system. These give the outputs for those actions and responses of the system, which take place despite any successful or failed authentication.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

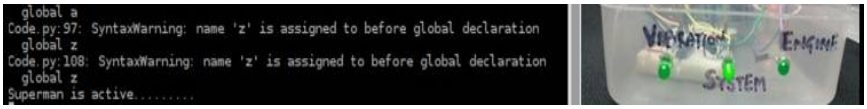


Figure 3. Output Screen and System LED showing system is turned on

Fig. 3 shows the outputs when the system connects itself to the internet and starts its functionality. It shows "Superman is active" when the SVATS is turned ON and hence the system LED (center) starts to glow.

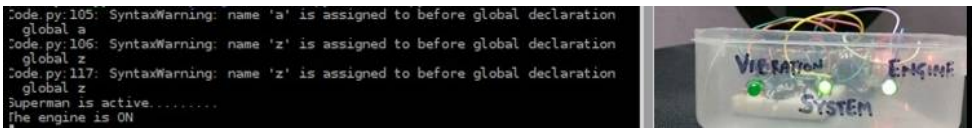
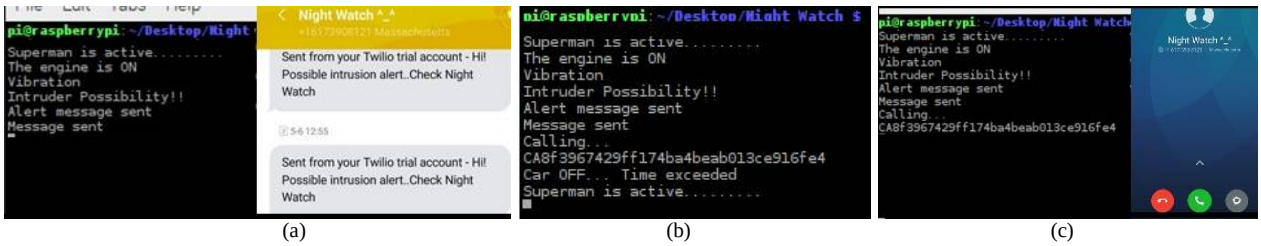


Figure 4. Output Screen and Engine LED showing the detection of ignition in vehicle

Fig. 4 shows the outputs when the system detects an ignition. It displays "The engine is ON" when it detects the ignition, making the Engine LED (right) to glow.

All the three parts of Fig.5 show the series outputs obtained after the system detects ignition of vehicle.



(a) (b) (c)

Figure 5. (a)Output and Mobile Screen showing an alert message to the owner (b) Output Screen showing the ignition was turned off after time exceeded to receive the password from the owner (c) Output and Mobile Screen showing an alert call made when no response was received in stipulated time

Fig. 5 (a)shows the outputs when the system on detecting an ignition, sends an online SMS alert to the owner with the message as "Possible Intrusion!! Check Night Watch". Fig. 5 (b) shows the output that says "Car OFF, Time exceeded" which is received when even after the alert call, there is no response from the owner. It assumes this a case of intrusion as the owner is not aware of it and hence not responding. Fig. 5 (c) shows the outputs the system doesn't receive a response in stipulated time and hence makes an alert call to the owner.

2. Successful Authentication

The output figures under successful authentication lay down those situations where the authentication of a user was a success. In such a scenario, a successful authentication can lead to either a positive response i.e. the password or a failed response i.e. any message but password from the user. Thus, parts in fig. 6 represent all such varied scenarios for successful authentication.

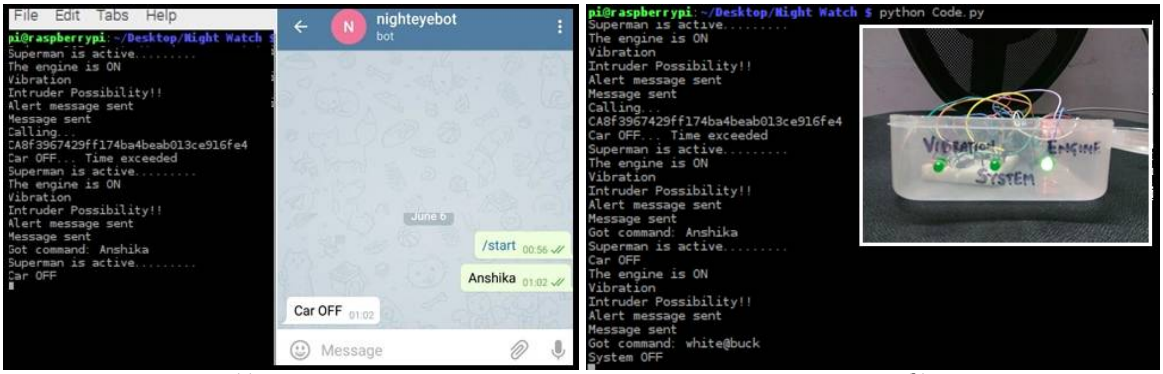
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017



(a) (b)

Figure 6. (a)Output and Mobile Screen showing the ignition was turned off in case of successful authentication but failed password (white@buck) match (b) Output Screen and led showing the system was turned off after successful user authentication and password match

Fig. 6(a) shows the outputs when the user responds which a message “Anshika” which is not the password, hence turning the ignition off as “Car OFF”. Fig. 6(b) shows the outputs when the user responds which a message “white@buck” which is the password, hence turning the system off as “System OFF” represented by System LED.

3. Unauthenticated Access

In case of unauthenticated access, when a response is received by the proposed system, it fails to authenticate the user as such a response, whether the password or any message, has been received from a stranger, unknown to the system. The following output i.e. fig. 7 represents the situation of unsuccessful user authentication.

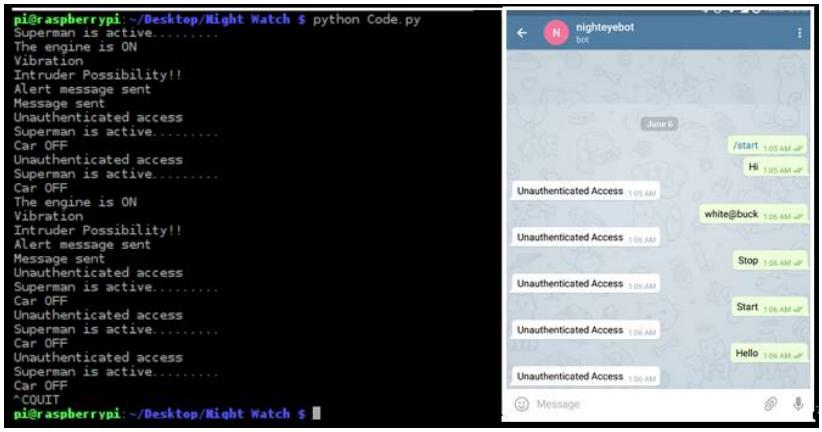


Figure 7. Output and Mobile Screen showing the ignition was turned off after unsuccessful user authentication whether password match or mismatch

Thus, fig. 7 shows that when such a situation is detected by the system, it turns the ignition off as “Car OFF” in the case of any response be it the password i.e. “white@buck” or any other type of message like “Stop, Start, Hi” etc.

VII. DISCUSSION AND CONCLUSION

The purpose of developing this system is mainly to introduce an inaccessible and advanced security system; a system that senses vehicle movement alerts the owner accepts owner’s commands and also responds automatically to a security threat. This proposed system aimed to be better compared to existing systems in the industry which merely either track the vehicle or just send information to the user but not take any action to actually prevent the theft.

It is comparably cost effective. The system is easy to use and learn due to its simple message and call alert feature. Users require no special training to use this proposed system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Fig. 3-7 show the effectiveness of the system. Thus, the system proposed in this paper proves to be an effective solution over the existing anti-theft systems in a user-friendly environment with ease of use and more security.

REFERENCES

[1] "A vehicle is stolen every 13 mins in Delhi", The Times of India, Available: https://goo.gl/RbL2yN, last accessed 2016/10/05.
[2] "Gone in 13 minutes: Vehicle thefts in Delhi break all records", The Times of India, https://goo.gl/taw2Do, last accessed 2016/10/07.
[3] Webb, B., "Steering Column Locks and Motor Vehicle Theft: Evaluations from Three Countries", Situational crime prevention: Successful case studies, 1997.
[4] Lee, S.J., Tewolde, G., Kwon, J., "Design and Implementation of Vehicle Tracking System Using GPS/GSM/GPRS Technology and Smartphone Application", IEEE Word Forum on Internet of Things, 2014.
[5] Laguador, J.M., Chung, M.M., Dagon, F.J.D, Guevarra, J.A.M., Pureza, R.J., Sanchez, J.D., Iglesia, D.K.I., "Anti Car Theft System Using Android Phone", International Journal of Multidisciplinary Sciences and Engineering, vol.4, no.5, pp.12-14, 2013.
[6] Wan, L., Chen, T., "Automobile Anti-Theft System Design based on GSM", International Conference on Advanced Computer Control, 2008.
[7] Boskany, N.W., Abdullah, R. M., "Intelligent Anti-Theft Car Security System based on Raspberry Pi 3 and GSM network", International Journal of Multidisciplinary and Current Research, vol.4, pp.538-541, 2016.
[8] Dutta, I., Gogoi, D., Gayan, B., Rabha, J., Katta, K., "A Review on Advanced Vehicle Security System with Theft Control and Accident Notification", International Journal of Current Engineering and Scientific Research, vol.1, no.3, pp.30-36, 2014.
[9] "ARM 7 Development Board", Available: https://goo.gl/LEm7qb
[10] Song, H., Zhu, S., Cao, G., "SVATS: A Sensor Network based Vehicle", INFOCOM: The 27th Conference on Computer Communications, 2008.
[11] Powale, P. K., Zade, G. N., "Real time Car Antitheft System with Accident Detection using AVR Microcontroller; A Review", International Journal of Advance Research in Computer Science and Management Studies Research Paper, vol.2, no.1, pp.509-512, 2014.
[12] "Bike Disc Lock", Available: https://goo.gl/y4PXGU
[13] "TK06", Available: https://goo.gl/SUdyhe
[14] "Airbag Steering Lock", Available: https://goo.gl/WoDGY9
[15] "Wheel Lock Clamp", Available: https://goo.gl/HX1DrQ
[16] "Clutch Lock", Available: https://goo.gl/1jpSEU
[17] "Anti-Theft IP Cam", Available: https://goo.gl/zr9UNS
[18] "What's ECU", Available:https://goo.gl/v7GXh1
[19] "Electronic Fuel Injection", Available:https://goo.gl/VqUswy