

IGuard: An Intelligent IOT based Security System for Server Rooms in Industries

Sagar Sawant¹, Jay Patel², Kiran Kokate³, N.K Kadale⁴

Student, Computer Department, NBN Sinhgad School of Engineering, Pune¹

Professor, Computer Department, NBN Sinhgad School of Engineering, Pune²

Abstract - IoT has provided a great opportunity to create powerful applications for industries with increasing demand of mobile phones, sensor devices and wireless application. In recent years there has been quite rise in industries among development in industrial systems and applications.

Key Words: Sensors, Bluetooth, IoT, Mobile Phone.

1. INTRODUCTION

In the recent years Internet of Things (IoT) is expected to offer solutions on transforming the role of many current industrial systems such as logistics systems and manufacturing systems. For example when IoT is used for creating industrial application for many industries like research and development medical science and engineering.

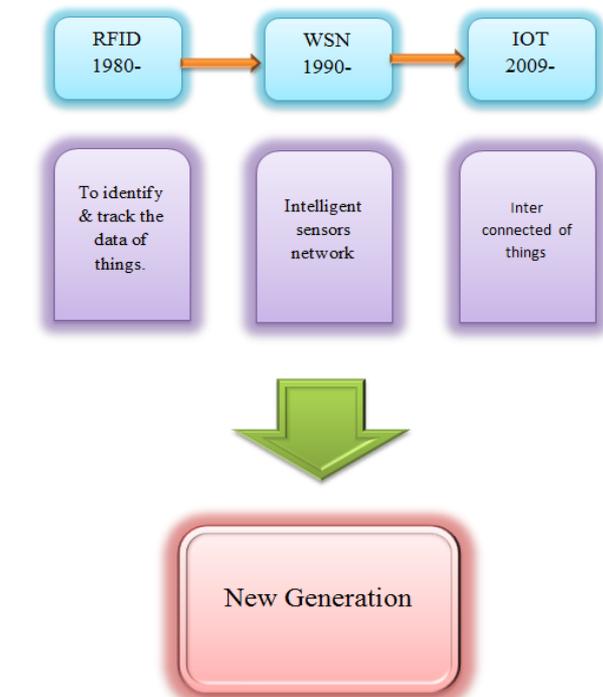


Fig-1: Related technology.

2. SYSTEM ARCHITECTURE

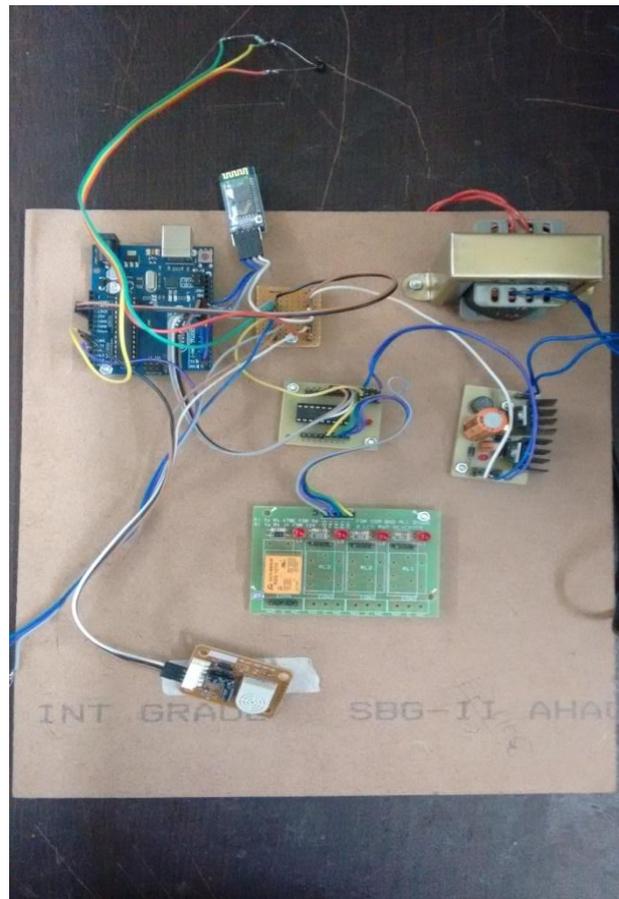


Fig-2: System Architecture

All living species contains biological sensors which functions similar to those of the mechanical devices described.

A sensor is a device that detects and responds to some type of input from the physical environment. The specific input could be light, heat, motion, moisture, pressure, or any other environmental phenomena.

3. SYSTEM GUI

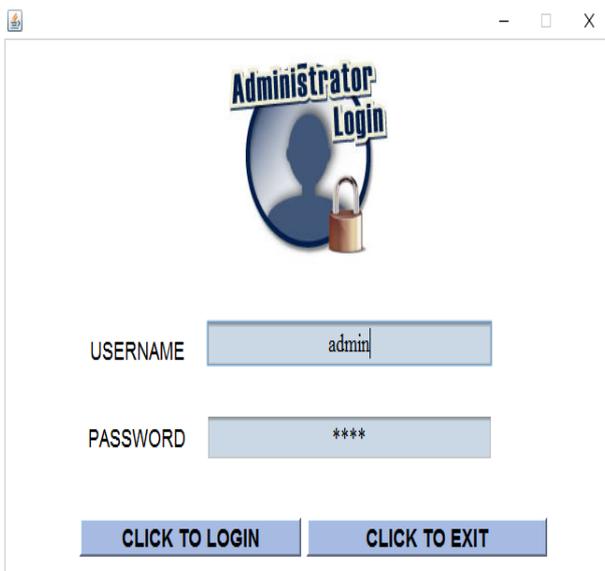


Fig -3: System GUI

This figure indicates that here Authentication will be going to check. To check the weather User/person is valid or invalid.

This will also ensure us that the person who doesn't have a valid Username & correct password wouldn't be able to get the access into the any type system.

In this figure we have given two options which are "click to Login" & "click to Exit" respectively.

These are credential which can and will be carried out by only one person that's called the Administrator.

He is only person in that organization that has the authority to check what is going on at any point of time he also can change something which is not going according schedule or going against organization policy. In this we have five options which

In case a user forgets his/her password or he/she find it difficult to memories it.

Which is common in now days so it can be easily changed to something which is more suitable or convenient to user as per there likes or dislikes.

The user/person who knows the correct old password can only able to change the password.

So the user who doesn't know the valid old password wouldn't able to change the password and he/she will be treat as invalid user to the system.

That when fault has been detected based upon that it will generate/send alters to the server and to concern person also.

With the help of camera which is present on that android device will detect the motion in that server rooms.

This will rectify that the some motion has taken places so they need to take appropriate action according to that so that they will reduce deficit.

4. SENSOR THRESHOLD

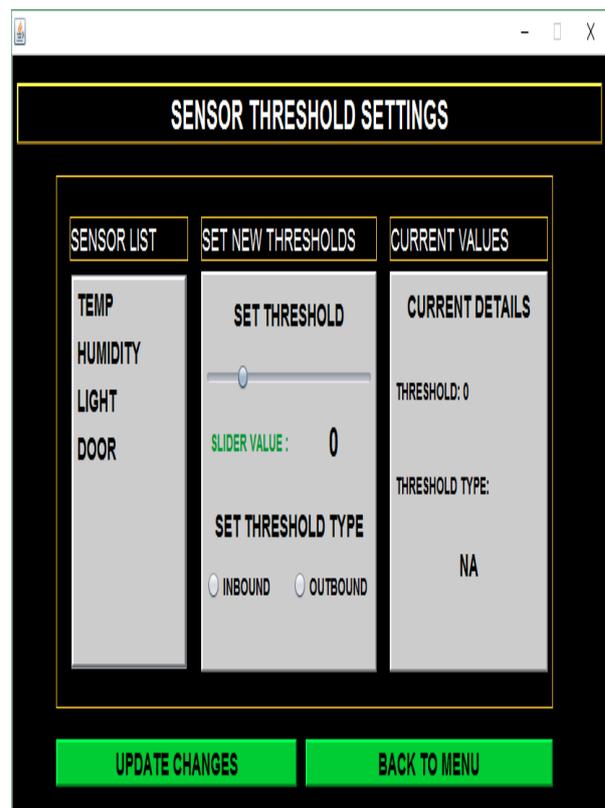


Fig -4: Sensor Threshold Setting.

This figure indicates that these sensors like temperature, humidity, light, door etc. The threshold value will be selected by the administrator that what should the value of threshold.

Inbound value means if the threshold value gets decrease by the set value it will generate alters and according to that proper action should/will be taken.

Outbound value means if the threshold value gets increase by the set value it will generate alters and according to that proper action should/will be taken.

5. Methodology

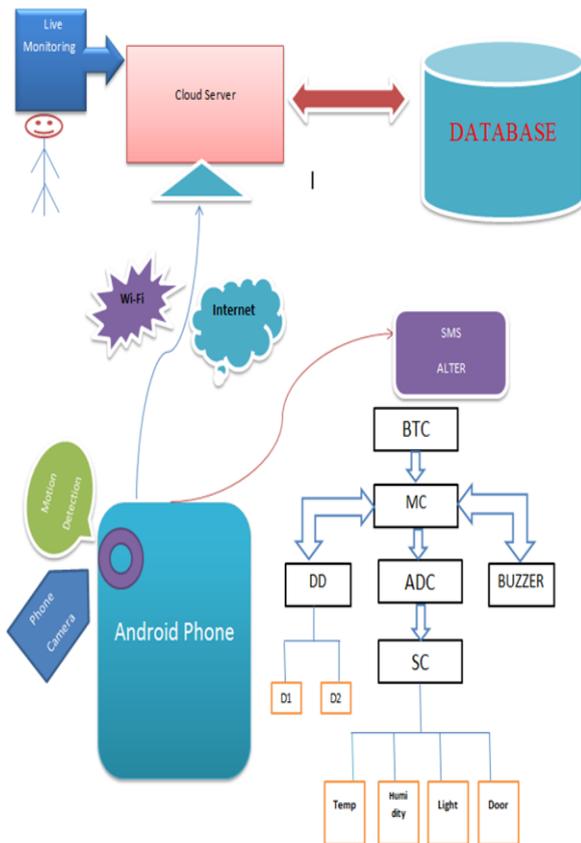


Fig -5: Block Diagram

In this system there is an android phone, with the help of Bluetooth controller it will connect through Bluetooth of that android phone. Through that Bluetooth it will connect through the micro controller then it will be connect through analog to digital converter. All the data will be live monitoring can be seen on the android device and in cloud server as well simultaneously.

It contain different devices drives & signal conditioning which has different sensors like door, light, temp, humidity etc. through them we can sense various inputs which will be given to signal conditioning so that they will perform their task.

If any misshaping happens then it will generate buzzer/alter in the form of short message services (sms) so to find the solution of that problem. It will be carried forward to the concern person (authority).

When fault has been detected based upon that it will generate/send alters to the server.

With the help of camera which is present on that android device we will detect the motion in that server rooms. It will rectify that the some motion has taken places so they need to take appropriate action according to that so that they will reduce deficit.

The data will send from that android device through Wi-Fi/internet to cloud server. All the data will send will be saved in the database. Where there will be a person who is keeping a close eye on the live monitoring. He can also generate/send alter manually if he see something is not right. So based upon the fault detect that he detect he can/will send the message to concern authority they will take action according to handle the situation.

In android devices there will be an application which will be there to see what is happening in that server rooms to keep it secure. This will also monitor what is happening there inside that room. When fault has been detected based upon that it will generate/send alters to the server. With the help of camera which is present on that android device we will detect the motion in that server rooms.

Monitoring the situation in a Server room in which data can see on Android mobile phone as well as from cloud server also i.e. Live Monitoring (including different sensors are available like temp. door, humidity, Light etc.) & all the operational data will be saved on the Database.

Presence of human or absent can be sense by the different sensors which are there to detection motion & then it will be carried out by Camera which is present in Android mobile Phone.

6. LIVE MONITORING

Basically live Monitoring means monitoring of activities and all the will data stored in the data base or data will transfer over networks such as the Internet. The monitoring is often used to by the governments, criminal organizations, corporations and individuals.

There is an android phone, with the help of Bluetooth it will connect to the hardware which also has Bluetooth for Bluetooth interfacing. Name of that Bluetooth is HC-05 and

if it's not paired before than it will scan for that device name so it will get that hc-05 bluetooth.

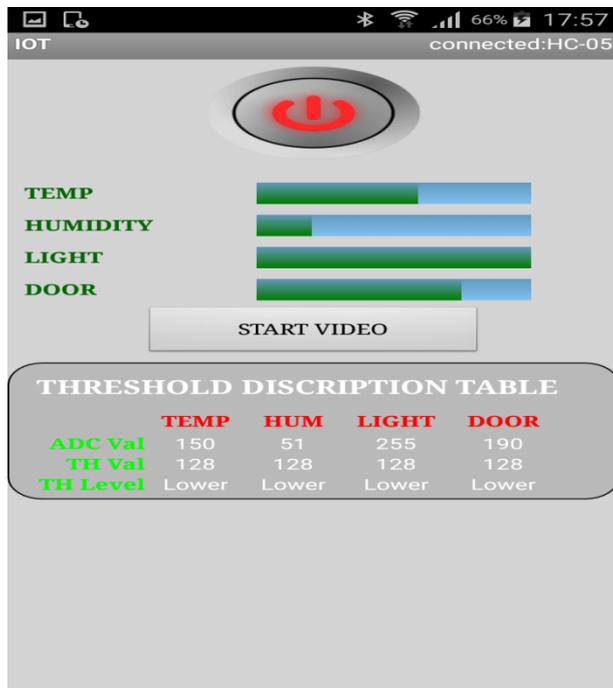


Fig -6: Android GUI.

In this we have used different types of sensors for sensing the information/data from physical world to feed it to the hardware.

Types of sensors are Temperature, humidity, light, door etc.

In those sensors the maximum value that can be read is 255 and the minimum value is 0 which is initial value before starting the device.

7. CONCLUSION

We provide high security for server rooms in industries with help of different sensors like temperature, humidity, light, door etc. we came to conclusion that our system is much better than the other system that we have in industries now a todays. Because we have provided additional function to our system like live monitoring, Motion detection etc.

The Internet of Things is closer to being implemented than the average person would think. Most of the necessary technological advances needed for it have already been made, and some manufacturers and agencies have already begun implementing a small-scale version of it.

8. REFERENCES

- [1]. D. Surie, O. Laguionie, T. Pederson, "Wireless sensor networking of everyday objects in a smart home environment", Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing-ISSNIP- 2008, pp. 189 – 194.
- [2] D. Evans, "The internet of things - how the next evolution of the internet is changing everything," White Paper. Cisco Internet Business Solutions Group (IBSG), 2011.
- [3] "Basis Tells Customers to Stop Wearing Its Peak Watch," 2016, <http://www.consumerreports.org/fitness-trackers/basis-tells-customers-to-stop-wearing-peak-watch>.
- [4] A. Rane, C. Lin, and M. Tiwari, "Raccoon: Closing Digital SideChannels through Obfuscated Execution," in 24th USENIX Security Symposium, J. Jung and T. Holz, Eds., 2015, pp. 431–446.
- [5] J. Clarke, R. Castro, A. Sharma, J. Lopez, and N. Suri, "Trust & security RTD in the internet of things: Opportunities for international cooperation," in Proc. 1st Int. Conf. Security of Internet of Things, Kollam, India, 2012, pp. 172–178.
- [6] L. Xu, "Introduction: Systems science in industrial sectors," Syst. Res. Behav. Sci., vol. 30, no. 3, pp. 211–213, 2013.
- [7] F. Li, C. Jin, Y. Jing, M. Wilamowska-Korsak, and Z. Bi, "A rough programming model based on the greatest compatible classes and synthesis effect," Syst. Res. Behav. Sci., vol. 30, no. 3, pp. 229–243, 2013.
- [8] Y. Lin, X. Duan, C. Zhao, and L. Xu, Systems Science Methodological Approaches. Boca Raton, FL, USA: CRC Press, 2013
- [9] L. Atzori, D. Carboni, and A. Iera, "Smart things in the social loop: Paradigms, technologies, and potentials," Ad Hoc Netw., to be published.
- [10] L. Xu, "Information architecture for supply chain quality management," in Int. J. Prod. Res., vol. 49, no. 1, pp. 183–198, 2011. [11] J. Z. Sun, "Towards the web of things: Open research issues and the BASAMI use case," Lect. Notes Electr. Eng., vol. 144, pp. 1–8, 2012.