International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Software Defined IoT(SD-IoT)

S.Naga Sowmya Sri [1]
M.Sc.(Computers)
Bhavan'sViveknanda College
Sainikpuri, Hyderabad,
Telangana State, India

N.Satya Shravani [2]
M.Sc.(Computers)
Bhavan'sViveknanda College
Sainikpuri, Hyderabad.
Telangana State, India

Ch.Rajagopal [3]
B.E (E.C.E), S.R.K.R Engineering College.
Bhimavaram.

Abstract:
Internet of Things (IoT) has recently received a great attention due to its potential and capacity to be into any complex system. The Encapsulate the control layer controls and implementation of service layer. The control layer preserves the sensor controller, network controller cloud control. We also discuss about functions control layer and service layer. My paper provides the modification for the existing security methods.

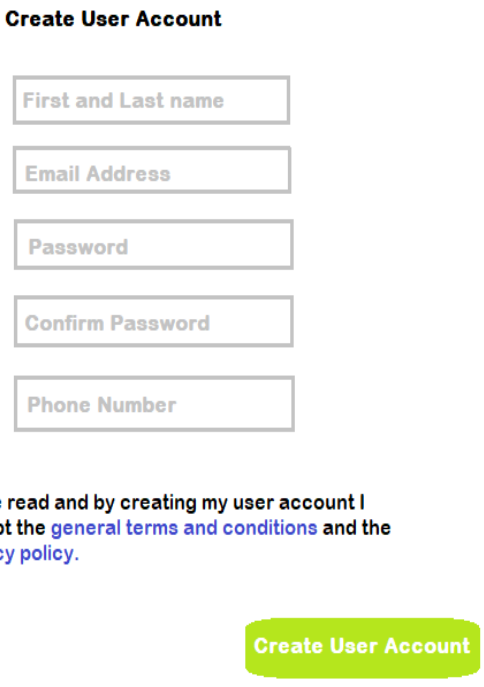
I -*INTRODUCTION:*

A new smart security feature that helps in accessing all electronics equipment remotely with high security password .It can access the entire home easily. It also helps in monitoring the devices .We can also know the status mode of that device in much secured manner .Authentication can be shared by only few members and they can handle the entire home appliances easily.

II- ANALYSIS:

The existing style of password is 'Text Password', 'Biometric', 'Voice Recognition'. This following password systems are also having some drawbacks.
People often choose their Name, Username, Telephone number, or some variant as their password. They choose the name of family members or friends, Pets vice versa. If we know all these details we can easily cracks the password. While coming to Bio metric, only authorised person can access the password. In humidity or moisture countries, it cannot recognise the finger prints because of their climate conditions. If the authorised person voice is mimic then they can crack the password of Voice Recognition. So we came up with an idea of implementing a new Security feature condition a new style of password is created with the name 'SSR security pattern' (Smart Security Random).

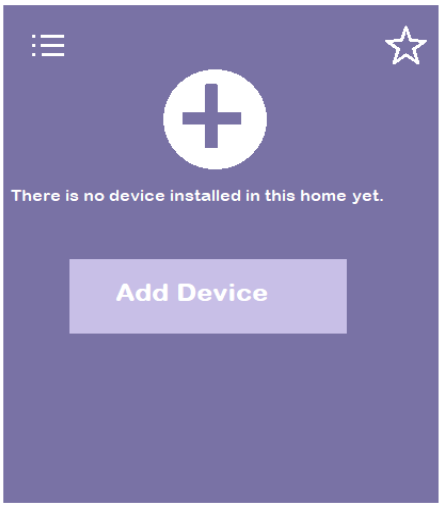
III - DESIGN: This is a platform independent. It can be a Web Application or App in Android, IOS store, Windows. This is a high security 'Style of Password'. This Iot App is developed to access all the household electric/electronic equipment .All the devices are connected to single wifi connection. We can access all the components in our smart phone / tab/ Smart watch.

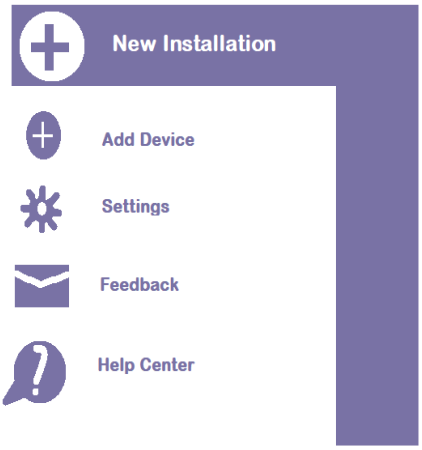


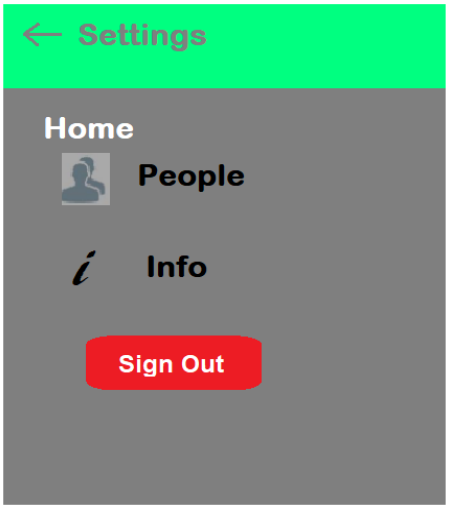
It displays all the devices which are connected and displays the current position of the devices (on/off state) if the appliance is in On mode then it changes its colour Red or else it has no colour. Once this gets implemented, all the devices can be handled by the person who is having authorization/ permission for accessing this Home page is following

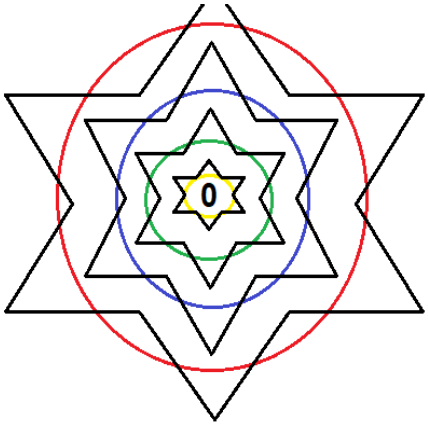
International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Login Page. Email id and Password should be match to access the Home page.

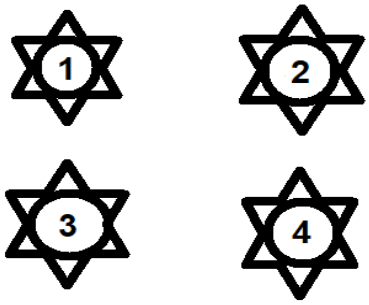








Design 1



Design 2

HOME PAGE: The Left-Top corner of the page contains "Tap-Icon". The Right-Top corner of the page contains "Security-Icon". When we click Top-Icon it extend to a new page which consist of Add Device, Settings, Feedback, Help centre.

If we click on Adding Device helps to install all the home made electronic equipment's we can add new home appliances. By using Setting Option we can add two permanent users and two temporary users to access through IoT. Help centre will help the customer to send his queries to the Customer Care team. Feed Back will help the developer to modify the features easily based on the suggestions/feedback given by the customer. Once all the devices are installed we can easily use this technology.

SECURITY ICON: Security Icon on the Right-Top corner on the Homepage. There will be a security window opening contains "SSR security pattern" (Smart Security Random). It contains two types of security patters which is designed in two different ways. One is for high security while another is for normal security.

Normal security feature consists of four Circles. One digital board which shows numbers will be place in the middle of the circle. When the user/ the customer need to rotate the four rings to set the password it contains only "Numerical values". Once he conform the password he needs to click on the submit button where his password will be saved in the Cloud Network.

High Security here we will display the four circles where user or the customer can easily adjust the ring to set the password. Once he conform the password then it is saved. It should contain one "Numeric" value one "Alphabet" value and one "Special character".

Once the first Password matches then second circle will be enables to rotate. In this manner customer has to rotate all the four circles till it matches the password. When the security password is matched it opens into the Home page.

PASSWORD reset:* Incorrect attempts of PASSWORD will ask for resetting.

For resetting:

1. Secret question
2. Email ID confirmation.
3. Mobile number OTP.

Once he finishes all these three steps, customer can reset his PASSWORD.

If it fails entire system gets locked. More than three wrong attempts lead to BLOCK THE LOGIN. It also captures the picture of the person and sends the alert message to the authenticator.

UNAUTHORIZED ACCESS:

1. When unknown person connects to your wifi and try to access your security feature. Once he turns the ring for entering the PASSWORD. When he fails to do it in two attempts for arranging first letter/number, System will alert the authorised person by sending notification to your phone and sending the picture of the unknown person.
2. As per security reasons/policies the security system will be blocked.
3. Authorisation persons only can access and resets the PASSWORD.

Advantages:

1. Easily to access entire house by using single app.
2. Easy to monitor (Current position of device).

Example:

1.If your in kitchen , need to know current position of AC(on/off) in your child's room. Yes it's very easy with this technology. You can easily access without going to that room.

2. When you are coming from the office and you need to switch on the heater/ AC. It can be easily done by using this technology.
3. Because of this security feature only the authorised person has access to control/monitor the devices.
4. Not an easy to crack this code as it sends continuous notification which alerts the authorised person.
5. Highly secured.

Future Scope:

This security feature can be implemented @ offices/houses. This can also be implemented @ door steps in corporate offices/RBI banks/ private sectors. So authorised persons only can enter the premises.

IV - *CONCLUSION:*

Smart house with a smart feature. An easiest way to handle all the devices within the house. Easy to monitor. It can also helps in saving electricity. As technology going smarter. We need to move in a smarter way. This technology helps us to handle entire house in smarter way.

Reference : References

[1] M.Karolin1, Dr.T.Meyyapan,"RGB Based Secret Sharing Scheme in Color Visual Cryptography", *International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015*

[2] Kirti Rawat , Vijay Kumar Joshi, Visual Cryptography for Grey Scale Images, International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2, Mar – Apr 2017

[3] M PavanKumar, G R RamaDevi, M V Ramana Murthy, A Paradigm to Provide A Secure and Sensitive Ad Hoc Networks, International Journal of Applied Engineering Research (IJAER), Volume 10, Number 1 (2015) *Special Issues*

[4] Gipsa Alex1 , Benitta Varghese2 , Jezna G Jose3 , AlbyMol Abraham4, A Modern Health Care System Using IoT and Android, Gipsa Alex et al. / International Journal on Computer Science and Engineering (IJCSE), 2014.

[5] Kirti Rawat , Vijay Kumar Joshi, Visual Cryptography for Grey Scale Images, International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2, Mar – Apr 201

[6] N Bhaskar, M V Ramanamurthy, "Big Data: Data Warehouse and Security", International Journal of Information Technology and Computer Science Perspectives, Pezzottaite Journals, ISSN: 2319-9016 (Print), ISSN: 2319-9024 (Online), Volume 6, Number 1 (January to March, 2017), pp. 2394-2400.

[7] Kavita Ahuja, and N.N.Jani, A STUDY OF TRADITIONAL DATA ANALYSIS AND SENSOR DATA ANALYTICS, International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016.

[8] Bhavani Thuraisingham, "Secure Sensor Information Management and Mining ", IEEE Signal Processing Magazine, 1053-5888, May 2004.

[9] Dr. Deepti Gupta, Wireless Sensor Networks 'Future trends and Latest Research Challenges', *IOSR-JECE , e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 2, Ver. II (Mar - Apr.2015)*