SECURING AUTOMATED OFFICE USING ADVANCED SECURITY METHODOLOGIES

Kshitij Halankar[1], Aditya Tembulkar[2], Kushal Vartak[3], Ankush Hutke[4]

[1 2 3]Student, Information Technology, Rajiv Gandhi Institute of Technology, Maharashtra, India
[4] Faculty, Information Technology, Rajiv Gandhi Institute of Technology, Maharashtra, India

ABSTRACT

Abstract— In recent years, internet use is increased tremendously. Many devices such as smartphones and laptops are constantly connected to the internet daily for a long period of time. Also the Internet of things(IOT) has gained importance due to its wide range of applications. Therefore, many industries are acquiring IoT in their offices. Devices used in IOT such as sensors transfer data over the network all the time. This data is sensitive information. If this information is leaked, there might be a large threat to the industry. Therefore, Security and privacy issues occur in IOT which have been described as the most challenging problems in the IoT domain. We propose an Automated office system as a module for implementing secure data transfer over the network.

The system controls fans and lights by constantly detecting temperature of the room and light present in the room. If the system detects smoke in office premises it sets the alarm off. If any intrusion is detected, the alarm is set and a notification is sent to the owner's mobile app. To enter the office the user needs to enter the password and after 3 unsuccessful attempts the alarm is set.

In order to secure the data transfer between sensors and devices connected to the network, the data is encrypted with AES encryption, so that the data cannot be accessed by any unauthorized user. Server authentication is secure by 3 level kerberos authentication which uses MD5 and AES for ticket generation. Server maintains log of the data transferred on the network. This log is encrypted using Blowfish algorithm. This paper presents the design and implementation of one such system, Secure Office Automation system.

Keywords: *Secure office automation, Internet of Things (IoT), Wi-Fi.*

1. INTRODUCTION

By 2020, it is estimated that the number of connected devices is expected to grow exponentially to 50 billion. The main driver for this growth is not human population; rather, the fact that devices we use every day (e.g., refrigerators, cars, fans, lights) and operational technologies such as those found on the factory floor are becoming connected entities across the globe. This world of interconnected things - where the humans are interacting with the machines and machines are talking with other machines is here and it is here to stay.

The Internet of Things (IoT) can be defined as a pervasive and ubiquitous network which enables monitoring and control of the physical environment by collecting, processing, and analyzing the data generated by sensors or smart objects.

And such increasing level of attention to IoT also introduces to the drawbacks that intruders use to gain unauthorized access. If an intruder is able to gain access to the sensitive information of an organization, then the organization may become vulnerable to many threats. Therefore, security is the main concern of the IoT today. We focus on making a system that helps to prevent many of such security attacks by providing various security mechanisms.

Most of the employees today spend all their work hours in their respective offices. Therefore the need of making an office more interactive and attractive is increasing rapidly. And due to the emphasis given to IoT, the implementation of IoT in Automated office is preferable by many people. But this increasing need also defines a set of new security threats to the office. Therefore an Automates Office System with better security mechanisms is mostly preferred.

2. LITERATURE REVIEW

The silver lining is that IoT security, previously ignored, has now become an issue of high concern, even at the federal government level. Several measures are already being taken to gap holes and prevent security breaches at the device level, and efforts are being led to tackle major disasters before they come to pass.

After the Jeep Cherokee hack, automaker Fiat scrambled to have the problem fixed and quickly issued a safety recall for 1.4 million U.S. cars and trucks to install a security update patch. The whole episode also served as a wakeup call for the entire IoT industry.

Now security firms and manufacturers are joining ranks to help secure the IoT world before it spins out of control. Digital security company Gemalto is planning to use its experience in mobile payments to help secure IoT devices. Gemalto will be offering its Secure Element (SE) technology to automotive and utility companies. SE is a tamper-resistant component that gets embedded into devices to enable advanced digital security and life-cycle management via encryption of and access-control limitation to sensitive data.

Microsoft also is entering the fray, and has promised to add BitLocker encryption and Secure Boot technology to the Windows 10 IoT, the software giant’s operating system for IoT devices and platforms such as the Raspberry Pi. BitLocker is an encryption technology that can code entire disk volumes, and it has been featured in Windows operating systems since the Vista edition. This can be crucial to secure on-device data. Secure Boot is a security standard developed by members of the PC industry to help make sure that your PC boots using only software that is trusted by the PC manufacturer. Its implementation can prevent device hijacking.

3. COMPARISON OF VARIOUS TECHNOLOGIES FOR OFFICE AUTOMATION SYSTEMS

Table 1: Comparison of various technologies for Office Automation Systems

IoT Software Platform	**Device management?**	**Integration**	**Security**	**Protocols for data collection**
2lemetry - IoT Analytics Platform**	Yes	Salesforce, Heroku, ThingWorx APIs	Link Encryption (SSL), Standards (ISO 27001, SAS70 Type II audit)	MQTT, CoAP, STOMP,M3DA
Appcelerator	No	REST API	Link Encryption (SSL, IPsec, AES-256)	MQTT, HTTP
AWS IoT platform	Yes	REST API	Link Encryption (TLS), Authentication (SigV4, X.509)	MQTT, HTTP1.1
Bosch IoT Suite - MDM IoT Platform	Yes	REST API	*Unknown	MQTT, CoAP, AMQP,STOMP
Ericsson Device Connection Platform (DCP) - MDM IoT Platform	Yes	REST API	Link Encryption (SSL/TSL),Authentication (SIM based)	CoAP

EVRYTHNG - IoT Smart Products Platform	No	REST API	Link Encryption (SSL)	MQTT,CoAP, WebSockets
IBM IoT Foundation Device Cloud	Yes	REST and Real-time APIs	Link Encryption (TLS), Authentication (IBM Cloud SSO), Identity management (LDAP)	MQTT, HTTPS
ParStream - IoT Analytics Platform***	No	R, UDX API	*Unknown	MQTT
PLAT.ONE - end-to-end IoT and M2M application platform	Yes	REST API	Link Encryption (SSL), Identity Management (LDAP)	MQTT, SNMP
ThingWorx - MDM IoT Platform	Yes	REST API	Standards (ISO 27001), Identity Management (LDAP)	MQTT, AMQP, XMPP, CoAP, DDS, WebSockets
Xively- PaaS enterprise IoT platform	No	REST API	Link Encryption (SSL/TSL)	HTTP, HTTPS, Sockets/ Websocket, MQTT

4. PROPOSED SYSTEM

The proposed system is designed to overcome limitation associated with existing system. Our system will provide security for IoT by providing secure encrypted communication between IoT devices and secure authentication mechanism for authenticating user.

Various sensors such as Temperature, Smoke, PIR, and Light are connected to Arduino UNO R3. A 16x4 LCD interface is connected to the Arduino. All the office appliances are connected to another Arduino through Relay switches. Arduino is connected to the wifi modem through the WIFI-ESP8266. The server computer and mobile apps are also connected to the same wifi network.

The various sensors connected to the arduino send the sensed data to the arduino. The data is then encrypted and sent to the server computer via the wifi network. The server computer decrypts and processes the data and sends the appropriate command which is in encrypted format to the arduino to which the office appliances are connected. The server computer contains a database in which the log file is maintained. If any security breach is detected by the server computer it will send a notification to the mobile app of owner.

The user who wants to enter to room must have to enter the password before entering into the room, once the user enters the room user has to login to the system within specified time to prove his/her identity. This helps to avoid unauthorized user from entering the room. If user fails to login to system then alarm goes off. Once user is successfully authenticated, the user can monitor the devices and appliances of the office. 3 level kerberos Authentication is used for the authentication.

The data sense by sensor is send to arduino, the arduino encrypt that data using AES algorithm. This encrypted data send then send over the network to other arduino to which devices or appliances are connected. while data is being transmitted from network the log of that data is created and the copy of that log file is stored into the database. This copy of encrypted data is encrypted using blow fish algorithm. Once the data is received by the Arduino, the Arduino decrypt that data and send appropriate command to the devices. The devices connected to arduino receives command and does assigned work.

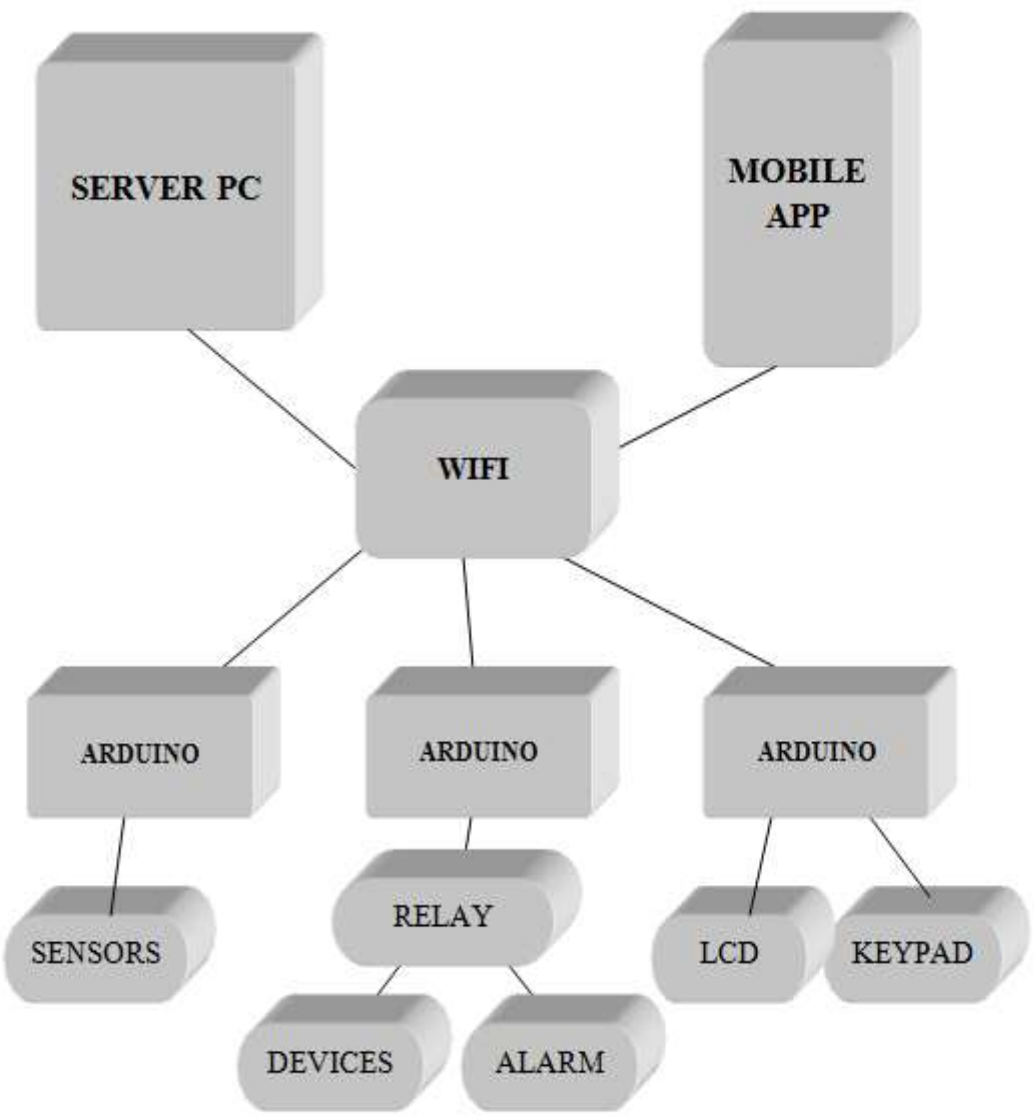


Fig 1:Block diagram For Advanced Security Methodologies In Iot Based Automated Office

The server maintain database that is used while authenticating user, the database also maintain log entries of each activity. this log can be used by owner for monitoring system. Both arduino are connected to same network.

The communication between IoT devices need to be secured to provide confidentiality for user data .In automated office the sensitive data of employee working in the office need to be protected. Many devices transmit data over the network, in many cases wifi is used for transmission. Therefore this transmission of data needs to be properly encrypted. Along with the transmission security, the database and the server also requires security. Therefore using a 3 level Kerberos authentication system to protect the data in database is necessary.

The hardware connections are shown in the figure 2. The first arduino is connected to a 16 x 2 lcd display through the data pins D13,D12,D11,D10,D9,D8. A 4 x 4 matrix keypad is used for input. It is connected on arduino pins D0,D1,D2,D3,D4,D5,D6,D7. If the user enters the wrong password 3 times, alarm goes off. The alarm is connected to the arduino on A0 pin.

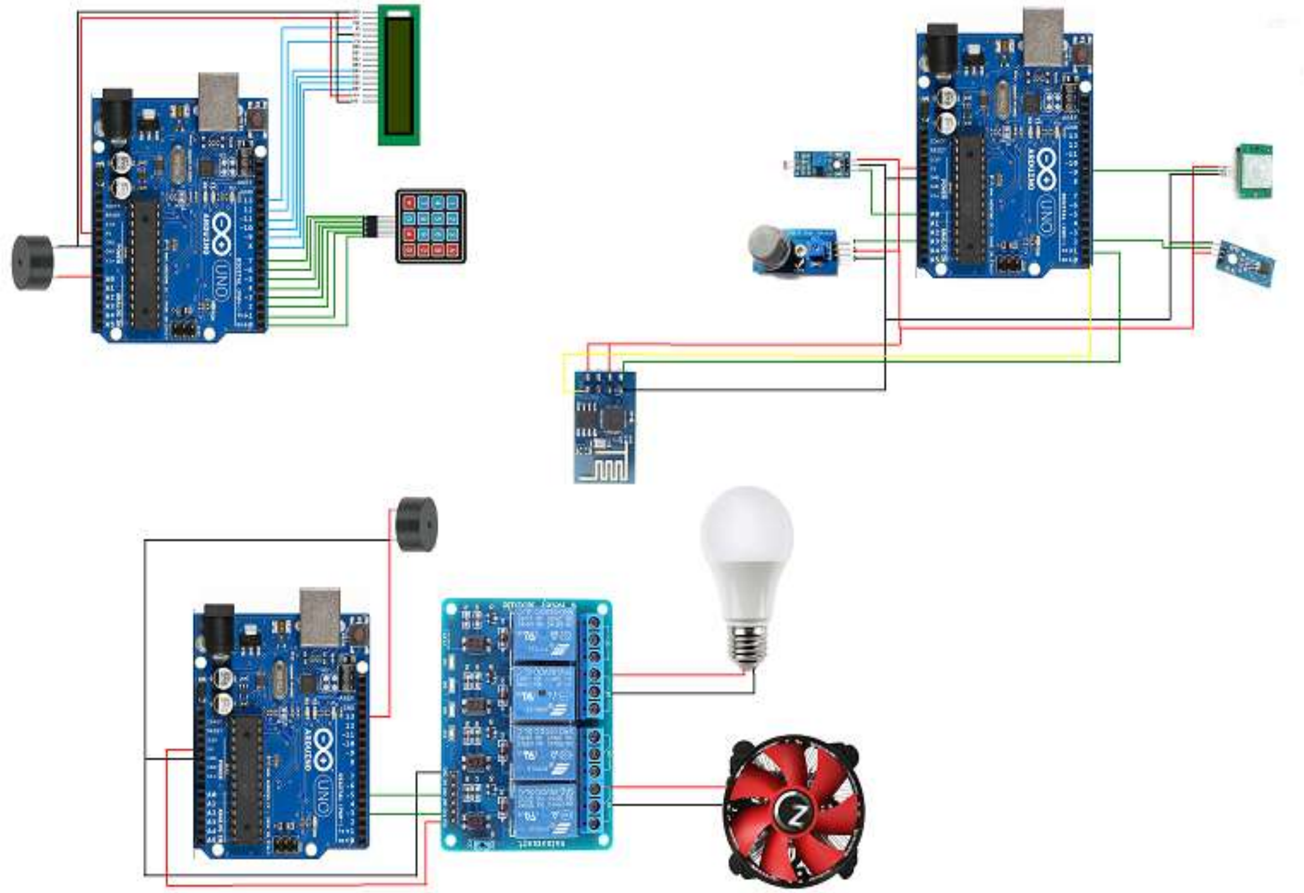


Fig 2:Hardware Connection For Advanced Security Methodologies In Iot Based Automated Office

The second arduino is connected to various sensors. The various sensors used are Temperature sensor, Gas sensor, Light sensor, PIR sensor. The temperature sensor is connected to the D2 pin of Arduino. The PIR sensor is connected to the D8 pin. Gas sensor is connected to the A3 pin. And light sensor is connected to the A0 pin of arduino. A wifi esp8266 model is used for generating wifi hotspot. Its transmitter pin is connected to D0 and Receiver pin is connected to D1 pin of arduino. All the devices are connected to +5v pin of arduino for power supply.

The third arduino in the above figure consists of devices usually found in any office. In this system we use bulbs and fans as they are most commonly used appliances in any office. A relay board is used to connect the office appliances. relay board is externally connected to a 240volt power supply. The bulb is connected to arduino at pin D5 through relay and the fan is connected to arduino at pin D3. An alarm is also connected at pin D13 of arduino for intrusion alert.

The figure below shows the work flow of Secured automated office, In which the user who wants to enter to room must have to enter the password before entering into the room, once the user enters the room user has to login to the system within specified time to prove his/her identity.

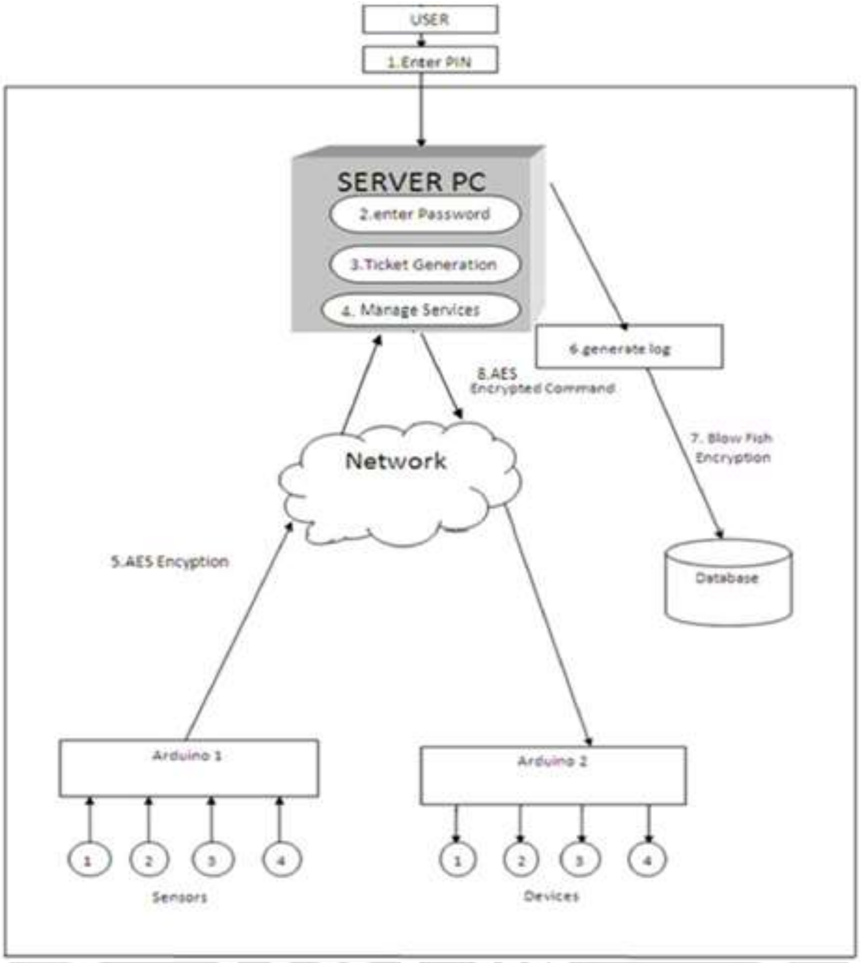


Fig 3: Workflow of Security Mechanism.

This helps to avoid unauthorized user from entering the room. If user fails to login to system then alarm goes off. Once user is successfully authenticated, the user can monitor the devices and appliances of the office. 3 level Kerberos Authentication is used for the authentication. The sensed data from sensor is send to arduino-1, the arduino-1 encrypt that data using AES algorithm. This encrypted data send then send over the network to other arduino to which devices or appliances are connected.

While data is being transmitted over network log of that data is created and copy of that log file is also created. This copy of encrypted data is encrypted using blow fish algorithm. Once the data is received by the arduno-2, the ardiono-2 decrypt that data and send appropriate command to the devices. The devices connected to arduino-2 receives command and does assigned work. The server maintain database that is used while authenticating user, the database also maintain log entries of each activity. This log can be used by owner for monitoring system. Both arduino are connected to same network.

5. IMPLEMENTATION

The actual working of the project includes the hardware specifications and sensors, power supply, Arduino, and software are NetBeans IDE, Android Studio, Arduino IDE, MySQL server.

5.1 Parameters used are shown in Table 2

Table 2: Parameters used in the project

Integrated Development Environment	NetBeans IDE, Android Studio, Arduino IDE
Micro controller	Arduino UNO R3
Clock Speed	16 MHz
Digital Communication Peripherals	1-UART
Input Voltage	5 volts
Programming Language	Java, android, Arduino

5.2 Hardware components

Hardware components include the Arduino UNO R3, ESP8266 Wi-Fi module, DHT11 temperature sensor, LDR LM393 light sensor, MQ2 gas sensor, Hc-Sr501 Passive Infrared motion sensor, 5 watt Bulbs and 12 volts computer Fans, Relay boards, 4x4 matrix numeric keypad, 16x2 LCD display, Piezo buzzers.

5.2.1 Arduino UNO R3

Arduino/Genuino Uno is a microcontroller board based on the ATmega328P. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

5.2.2 DS18B20 temperature Sensor

The DHT11 is a basic, ultra low-cost digital temperature and humidity sensor. It uses a capacitive humidity sensor and a thermistor to measure the surrounding air, and spits out a digital signal on the data pin (no analog input pins needed). It's fairly simple to use, but requires careful timing to grab data. The only real downside of this sensor is you can only get new data from it once every 2 seconds, so when using our library, sensor readings can be up to 2 seconds old.

5.2.3 LM393 light sensor

The LM393 works like a digital switch. Its output will be set to LOW or HIGH on the DO (Digital Output) pin. The sensitivity of this module can be adjusted by turning the built-in a potentiometer to the desired value. Due to the design of the module, it would be acting as a switch, as an analog pin is not available.

5.2.4 MQ2 gas sensor

The Grove - Gas Sensor(MQ2) module is useful for gas leakage detecting(in home and industry). It can detect LPG, i-butane, methane, alcohol, Hydrogen, smoke and so on. Based on its fast response time. measurements can be taken as soon as possible. Also the sensitivity can be adjusted by the potentiometer.

5.2.5 Hc-Sr501 PIR sensor

PIR（Passive Infrared Detection) Motion Sensor is usually used in the security field. All people can output infrared light. When somebody moves in front of the module, then the infrared light variation will be detected by the module. For this sensor, it will output a high voltage when people moves in front of it.

5.2.6 4x4 matrix keypad

The 4 X 4 Matrix Keypad is a very simple one which have 16 tactile keys connected to the male headers across the resisters on the same board. It is very small and easy to carry. Its simplicity is just to give the power to the keypad and connect the headers to the micro-controller's input port with 8 pin female connecting wire. When one tactile key is pressed its corresponding pin with Rows and column intersection gets high logic.

5.2.7 16x2 lcd display

LCD (Liquid Crystal Display) is used in all the electronics projects to display the status of the process. A 16x2 alphanumeric LCD is most widely used module of LCD nowadays. There are several others type of LCD available in market also.

5.2.8 Piezo buzzer

Piezo buzzer is an electronic device commonly used to produce sound. Light weight, simple construction and low price make it usable in various applications like car/truck reversing indicator, computers, call bells etc. Piezo buzzer is based on the inverse principle of piezo electricity discovered in 1880 by Jacques and Pierre Curie. It is the phenomena of generating electricity when mechanical pressure is applied to certain materials and the vice versa is also true. Such materials are called piezo electric materials.

5.2.9 Wi-Fi Module ESP8266

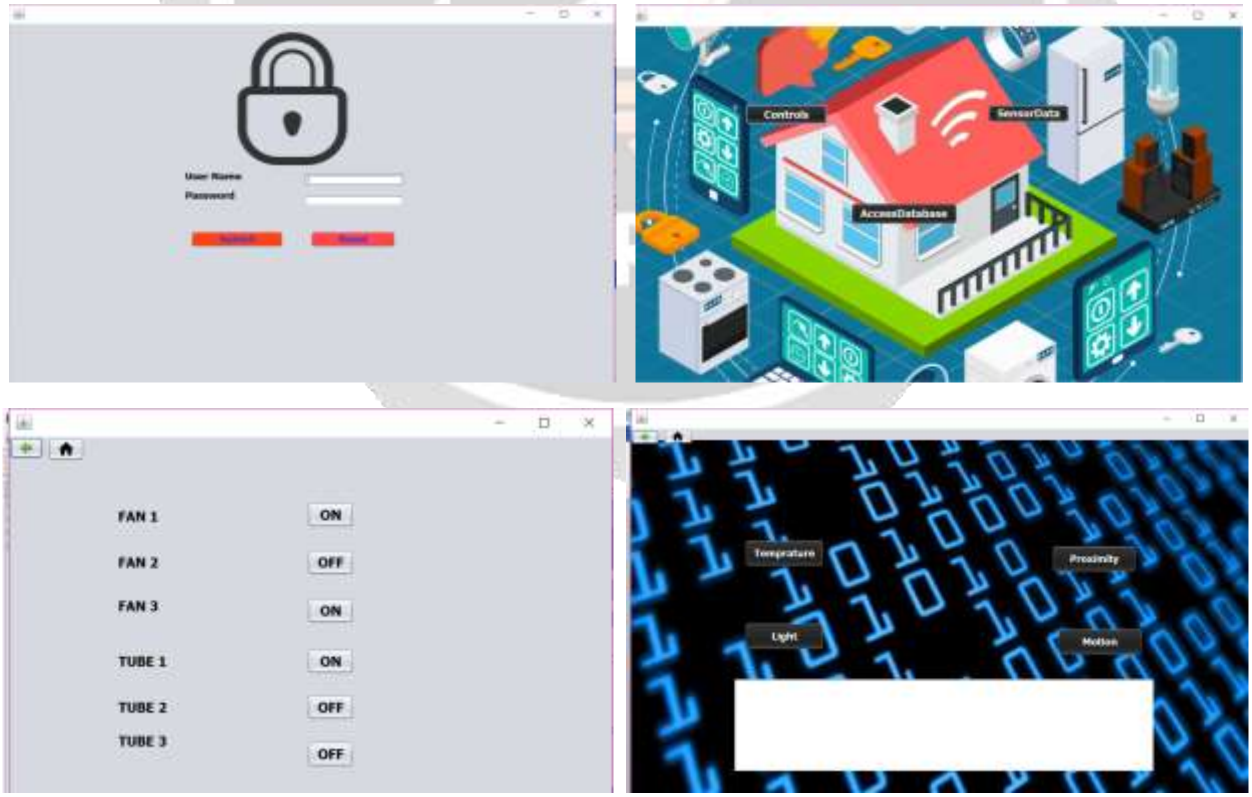
ESP8266 is a low cost Wi-Fi module which is perfect for giving WiFi functions to a microcontroller via a UART serial connection. ESP8266 can also be programmed to be a standalone Wi-Fi module.ESP8266 requires a 3.3V power supply. It can serve as a Wi-Fi adapter as well.ESP8266 operates in three modes: active mode, sleep mode and deep sleep mode. It can also be used to host Wi-Fi applications.

5.3 Software Components

Software components include a computer software to control the office appliances and a mobile app that notifies the changes happened in the office along with intruder alert.

5.3.1 Computer Software

The software was developed in java. It is connected to the database. For the back end we have used MySQL server. The java software has a 3 level kerberos authentication system for login. Once the user is logged in, the user has access to the database and control the office appliances. The database stores sensor data in blowfish encrypted format.

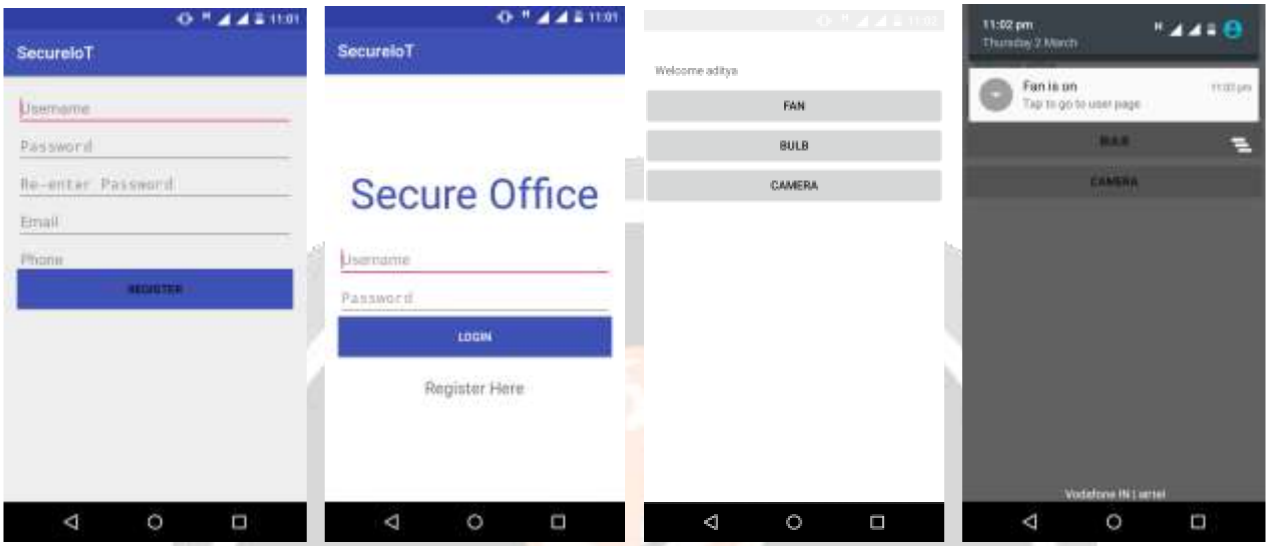


FAN 1 ON
FAN 2 OFF
FAN 3 ON
TUBE 1 ON
TUBE 2 OFF
TUBE 3 OFF

FIG.4: Server Software

5.3.2 Mobile App

The purpose of mobile app is to control office appliances. It acts as a remote control to quickly access devices installed in office. Its main purpose is to notify the owner of the office about any intrusion or unauthorized access to the office. If any intrusion is detected in the office the server software sends a notification to the app. Therefore quick actions can be taken. It also notifies if any state of the devices in office change such as if the fan is turned on a notification appears which says the fan is on.



Welcome aditya

Fan is on
Tap to go to user page

FIG.5: Mobile App

6. RESULT

We have developed the software and app and integrated them both with hardware over wifi network. It has led to a successful implementation of a system which automatically controls all the office appliances and provides security over the network.

7. CONCLUSION

The developed system has the ability to control the devices connected in office throughout the day, in any environment. The main feature of this system is secure data transfer. The system provides quick access to the office appliances without compromising the security. The authentication mechanism used in the system does not let any intruders break into system. As the data sent over the network is encrypted, if the wifi network is compromised the attacker cannot easily decrypt the information. The server software developed in java provides both manual and automated access to the office appliances. The mobile app receives notifications about any intrusion in just a few seconds. Hence the results provided by this system are real time therefore it can easily replace existing automation systems.

8. REFERENCES

[1] Appcelerator, Inc. (2015), Appcelerator Open Source.*http://www.appcelerator.org/*.

[2] Gazis, V.; Gortz, M.; Huber, M.; Leonardi, A.; Mathioudakis, K.; Wiesmaier, A.; Zeiger, F.; Vasilomanolakis, E. (2015), A survey of technologies for the internet of things, in Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International , vol., no., pp.1090-1095, 24-28Aug.2015

[3] Jasper (2014), Achieving End-to-End Security in the Internet of Things, *http://pages.jasper.com/White-Paper-Cellular-IoT-Security_Cellular-IoT-Security.html*

[4] LogMeIn (2015), A Guide To Designing Resilient Products for the Internet of Things, LogMeIn

[5] Louis Columbus (2015), Mattermark Lists The Top 100 Internet Of Things Startups For 2015, *http://www.forbes.com/sites/louiscolumbus/2015/10/25/the-top-100-internet-of-things-startups-of-2015/*

[6] Perera, S. (2015), IoT Analytics: Using Big Data to Architect IoT Solutions, WSO2 White Paper, *http://wso2.com/whitepapers/iot-analytics-using-big-data-to-architect-iot-solutions/*

[7] sWSO2, Inc. (2015), WSO2 Unveils Open Source WSO2 Data Analytics Server 3.0, Delivering Comprehensive Analysis Optimized for The Internet of Things, *http://wso2.com/about/news/wso2-unveils-open-source-wso2-data-analytics-server-3.0-delivering-comprehensive-analysis-optimized-for-iot/*

[8] WSO2, Inc.(2015), Open Platform for Internet of Things, *http://wso2.com/landing/internet-of-things/* Wijewantha, D.(2014), Demonstration on Architecture of Internet of Things - An Analysis, WSO2 Library Article, *http://wso2.com/library/articles/2014/09/demonstration-on-architecture-of-internet-of-things-an-analysis/*

[9] Wei Wu, Yong Huang, "The Analysis and Design of Office Automation System based onWorkflow", in *Electronic and Mechanical Engineering and Information Technology (EMEIT),2011 International Conference*, Volume: 1, Pages: 223 - 225, 2011.

[10] Di Libaier, "Enterprise office automation system design and implementation" in *Seventh International Conference on Measuring Technology and Mechatronics Automation*, Pages: 457 -461, 2015.

[11] Surapon Kraijak, Panwit Tuwanut,"A Survey On Iot Architectures, Protocols, Applications, Security, Privacy, Real-World Implementation And Future Trends" in *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015),*Pages: 1 - 6, 2015.

[12] Pranay P. Gaikwad, M. E. Student Jyotsna P. Gabhane, Snehal S. Golait, "3-Level Secure Kerberos Authentication for Smart Home Systems Using IoT", *2015 1st International Conference on Next Generation Computing Technologies (NGCT),*Pages: 262 - 268, 2015.

[13] Teng Xu, James B. Wendt, Miodrag Potkonjak, “Security Of Iot Systems: Design Challenges And Opportunities” in *2014 IEEE/ACM International Conference On Computer-Aided Design(ICCAD)*, Pages: 417 - 423, 2014.

[14] Arbia Riahi, Enrico Natalizio, Yacine Challal, Nathalie Mitton, Antonio Iera, “A Systemic And Cognitive Approach For Iot Security” in *Computing, Networking And Communications (ICNC),2014 International Conference,* Pages: 183 - 188, 2014.

[15] RwanMahmoud, TasneemYousuf, FadiAloul, Imran Zualkernan, ”Internet Of Things (Iot) Security: Current Status, Challenges And Prospective Measures” in *10th International Conference For Internet Technology And Secured Transactions (ICITST),* Pages: 336 - 341,2015.

[16] Mary R. Schurgot; David A. Shinberg; Lloyd G. Greenwald, “Experiments With Security And Privacy In Iot Networks” in *World Of Wireless, Mobile And Multimedia Networks(Wowmom), 2015 IEEE 16th International Symposium* Pages: 1 - 6, 2015.

[17] Ming Wang, Guiqing Zhang, Cheng hui Zhang, Jian bin Zhang, and Cheng dong Li, ”An IoT-based Appliance Control System for Smart Homes”, *Fourth International Conference on Intelligent Control and Information Processing (ICICIP)*, pp. 744-747, June 9 11, 2013.