Advanced Security Methodologies in IoT based Automated Office

Kshitij Halankar
B.E., Department of Information Technology
Rajiv Gandhi Institute of Technology
Halankarkshitij1@gmail.com

Aditya Tembulkar
B.E., Department of Information Technology
Rajiv Gandhi Institute of Technology
atembulkar@gmail.com

Kushal Vartak
B.E., Department of Information Technology
Rajiv Gandhi Institute of Technology
0kushal0@gmail.com

Ankush Hutke
Assistant Professor
Department of Information Technology, Rajiv Gandhi Institute of Technology
ankush.hutke@gmail.com

***Abstract*---**Over the years IoT has gained importance and the need of IoT is increasing rapidly. Internet is reaching every bit in the world. Many devices such as smartphones and laptops are constantly connected to the internet. Therefore, many industries are acquiring IoT in their offices. Due to the increasing need of IoT, Security and privacy issues have been described as the most challenging problems in the IoT domain. We propose an Automated office system that provides a secure approach for sharing the data between the IoT devices. The designed system is very effective and eco-friendly having the advantage of low cost. This system eases out the office automation tasks and user can easily monitor and control office appliances from anywhere and anytime using connected network. Various security algorithms and encryption are used which are explained later in the paper.

*****

I. 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 (M2M) — 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. The concepts and technologies that have led to the IoT, or the interconnectivity of real-world objects, have existed for some time.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 day by day. Although it is beneficial 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.

II. LITERATURE REVIEW

One new concept associated with the “Future Internet” is called “Internet of Things”. The IoT become a vision where real-world objects are part of the internet: every object is uniquely identified, accessible to the network, its position and status known, where numerous services and intelligence are added to effectively expand an Internet, seamlessly combining between the digital, physical world, eventually affecting on personal, social environment.[3].

With the increasing use of Internet of things number of devices connected to the internet are increasing. These devices are also becoming target for various security risks. The Internet of things has various security threats that must be also the part of automated office. There are various security issues like malicious code attack, tampering with node-based application, eavesdropping, sniffing attacks, noise in the data, unauthorized access and physical issues like physical damage, loss of power and Environmental attacks.

Using IP protocol will provide confidentiality, integrity, data origin authentication and protection. We will be using 2 IPSec protocol: Authentication Header (AH) and Encapsulated Security Protocol (ESP).

There are various technologies and methodology that are used to protect IoT from the various security issues mentioned above. Few of the issues will also be there in automated office. We will be using the respective solution from various sources and will apply them on automated office to make it more secure.

III. 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.

Figure 1 shown below is the work flow of Automated Office System. Various sensors such as Temperature, Proximity, 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 Wi-Fi modem through the Arduino Wi-Fi Shield. The server computer and mobile apps are also connected to the same Wi-Fi network.

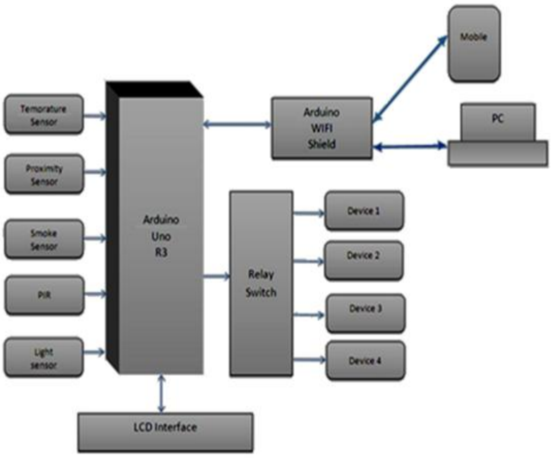

Fig 1: Workflow of Automated Office

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 Wi-Fi network. The server computerdecrypts 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. Arduino Wi-Fi shield provides connection interface between arduino and Wi-Fi modem. If any security breach is detected by the server computer it will send a notification to the mobile app of owner.

The figure 2 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,

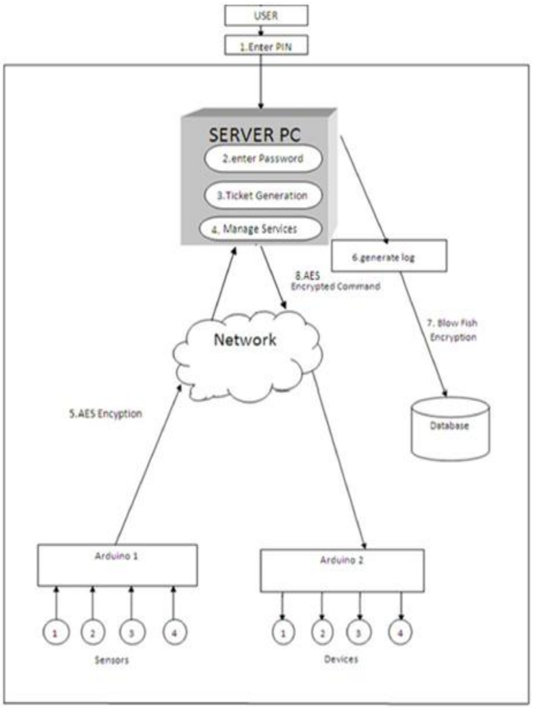

Fig2: Workflow of Security Mechanisms in Automated Office

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-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 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 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.

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 Wi-Fi 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.

IV. DESIGN

The implementation design and detail of our proposed system can be understood well with the help of the following data flow diagram. Along with the flow of the data it shows how data will be secured and

Stored to analyzed and take according action.

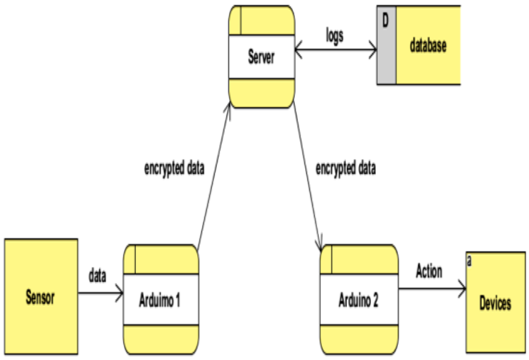

Fig 3. Level 0 DFD

From the below FIG Data Flow Diagram it is clearly visible that system contain two Arduinos, one arduino is used to get input from sensor, where as another arduino sends command to devices. The first arduino send data to server which is encrypted and then server send data to another arduino which is also encrypted.

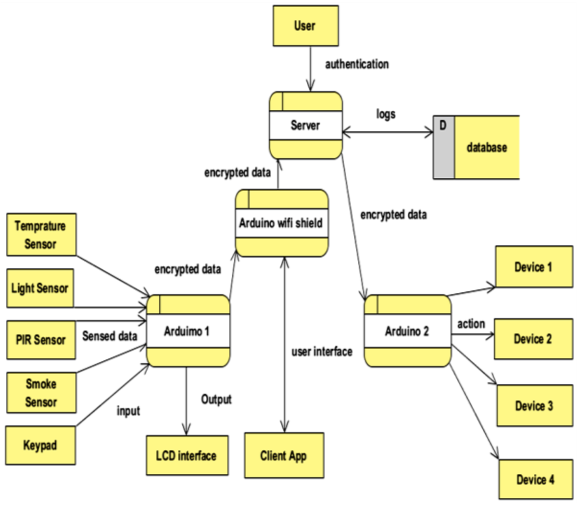

Fig 4. Level 1 DFD

The above figure shows that system handle multiple sensors as well as many devices. Whenever data comes from sensor to arduino the arduino encrypt that data and send that data to server .server decrypt that data create log of that data. While sending data to another arduino server encrypt that data using different algorithm. Once arduino receive that data it decrypt that data and send appropriate command to devices connected to it

V. CONCLUSION

In this paper we have seen and concluded that use of IoT is increasing. Various security issues are associated with automated office .Thus according to the issues identified we have proposed few solutions for it. We have summarized the limitations of the existing security methods and proposed future work recommendations to overcome these limitations. Inorder for the customers to embrace the IoT technologies and the applications, these privacy and security issues and limitations need to be addressed and implemented immediately.

REFERENCES

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

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

[3] 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.

[4] 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*

[5] *International Conference on Next Generation Computing Technologies (NGCT)*,Pages: 262 - 268, 2015.

[6] Sandip Ray, Swarup Bhunia,Yier Jin, Mark Tehranipoor, "Security Validation In Iot Space" in *2016 IEEE 34th VLSI Test Symposium (VTS)*,Pages: 1 - 1,2016.

[7] 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.

[8] Jacob Wurm, Khoa Hoang, Orlando Arias, Ahmad-Reza Sadeghi, Yier Jin, "Security Analysis On Consumer And Industrial Iot Devices" in *21st Asia And South Pacific Design Automation Conference (ASP-DAC)*, Pages: 519 - 524, 2016.

[9] Arbia Riahi, Enrico Natalizio, YacineChallal, 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.

[10] 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.

[11] 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.

[12] Dietmar P.F. Mller, Hamid Vakilzadin, "Wireless Communication in Aviation through the Internet of Things and RFID", pp. 602-607, 2014.

[13] Sean Dieter Tebje Kelly, Nagender Kumar Surya devara, and Subhas Chandra Mukho padhyay, "Towards the Implementation of IoT for Environmental Condition Monitoring in Homes", *IEEE Sensors Journal*, Vol. 13, No. 10, pp. 3846-3853, October 2013.

[14] 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.

[15] Moataz Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou, and Chung-Horng Lung, "Smart Home: Integrating Internet of Things with Web Services and Cloud Computing", *IEEE International Conference on Cloud Computing Technology and Science*, pp. 317-320, 2013.