Server Room Access Control Using (IOT)

LEENA KOLHE [1], SUVARNA MORE [2], KAJAL AHER [3], ASHWINI THAKARE [4]
[1,2,3,4] *Dept. of computer Engineering, Late G. N. Sapkal College of Engineering, Nashik*

Abstract -- This concept contains the architecture and implementation of an Internet Of things based mobile application for a Server room access control security system. This implementation has two devices i.e. Mobile and the Door, both are connected to the internet. The sensors are connected to the internet (IOT) to be monitored remotely from anywhere in the world. This system save log of door status information i.e. the lock unlock information is saved on the sever and is displayed on the mobile application. The application also includes several other security features to enhance the security level and make the key management process easy.

Indexed Terms -- Internet of Things (IoT), Smart lock, Android Application, Lock log, Access control, Hashid Encoding & Decoding, AES Encryption & Decryption.

I. INTRODUCTION

The technology of keys and locks remained the same for the last century while everything else is evolving exponentially. So why not use current technologies and apply it with old ones to build something new and innovative. Around 4000 years ago, the concept of Locks and Keys were invented, and until today, regardless of some minimal variation in security and sustainability, locks are installed in doors stimulated mechanically by the right key.

Recently, the Internet was enhanced, and everything was connected to it (phones, televisions, laptops, tablets, cars and so on…). This was done because we wanted to make systems "smarter", in other term "more productive". Why not do the same thing with Locks? Enhancing the locks mechanism by connecting them to the internet, making them more robust and productive. Today, the number of mobile device users including Smartphone users has rapidly been increasing worldwide, and various convenient and useful Smartphone applications have been developed [2]. Now smart phones are not only used to send and receive phone calls, send text messages, and perform mobile banking operations, but they also are used to control various other devices in our real everyday lives. Through a mobile operating system and internal applications, we can remotely control a variety of external devices such as TVs, projectors, computers, cars, etc.

People normally operate ordinary locks with keys or keyword locks such as a pin code. However, these locks have few drawbacks such as misplacing keys or forgetting passwords. Using smart phones, the remote lock can be easily managed. Furthermore, the proposed system has wide range of applications and can be used for various types of locks and systems, such as lockers, bicycles, cars, etc.

Smart-Lock-System is a complete reinvention of the standard Key-Door lock, where all the digital keys are stored in a Digital Keychain kept on the owner's phone.

Encrypted and secured Smart-Lock-System can be connected to the Internet via internet cable (UTP) or wirelessly (Wi-Fi).

II. RELATED WORK

Electronic door locks have been a popular mechanism to enforce physical access security in the enterprise for close to four decades. It allows the maintenance staff to issue keys i.e. access cards, revoke them remotely and also control access to the specific sections of a building. For example, when employees unauthorized to access a sensitive section of the building use their cards to access it, the maintenance staff gets alerted with the identifying information of the miscreant, area being accessed, and the time at which the infraction happened. Such deployments needed heavy investments of infrastructure, software, and maintenance staff which drove up the deployment cost prohibiting their usage for regular home settings. The average costs for having electronic access control for each door can be as high as $5000 [1]. The access

control systems can be a highly secure solution for the enterprise [2], but have not been affordable or suitable for home use.

However, the revolution in the IoT coupled with the proliferation of smart phones and cloud based technologies spurs the recent adoption of SDL for home and other commercial use. The SDL are an attractive replacement to traditional door locks as they offer increased security, and easy key sharing while offering ease of operation. The cost is not prohibitive for home usage, especially considering its benefits over a traditional door lock.

These smart lock systems can be categorized into three broad types based on their approaches - biometrics, smart tags, and smartphones. However the current solutions often pose issues of usability, reliability as well as security. Bio-metrics based smart door locks [3], [4] rely on the unique physical characteristics of humans such as fingerprints, face and retina to grant access to authorized users. Such biometricbased techniques can be easily spoofed and are hard to replace once compromised. In spite of advances like liveliness detection algorithms, biometric based techniques are prone to easy security breaches [5]. Existing smart tags [6] and smartphone SDL solutions [7], [8] utilize some form of wireless Radio frequency (RF) communication, such as Radio frequency Identification (RFID), Near Field Communication (NFC) technology, Wi-Fi, and Bluetooth. NFC and RFID have very limited transmission ranges that may constrain its usage for SDL applicaions. Moreover, they all operate in RF communication that is becoming very crunched in this IoT era, causing RF [9] and vulnerable to jamming and interference.

With the heavy proliferation of IoT devices, innovative usage of other communication channels in the optical and audio spectrum is bringing much needed relief to the RF spectrum [10], [11], [12]. These optical and audio spectrum channels may offer connectionless alternatives to the traditional RF based approaches. Within the optical channel, there are studies that achieve the communication by modulating visible light LED [13] to encode data bits that are received via an optical receptor of a smartphone or other IoT devices such as the camera or ambient light sensor. Within the audio channel, [11], [12] enable the communication by modulating the sounds waves to encode data bits that are received via the microphone of a smartphone or other IoT devices. When exploited for specific applications, the use of optical or audio spectrum results in a much efficient solution than increasing the reliance on RF technologies.

It is worth to note that traditionally IR communication has been used to control household devices such as TV remote and garage doors without programmability. Recently IR has been used to enable to efficient indoor localization [14], and disabling iPhone camera at concerts and movie theaters using IR receiver of a phone [10]. However, this work is unique in that we use a smartphone's IR emitter for controlling SDL with rich security schemes and programmability.

III. OBJECTIVES

- The main objective is to design secure lock using the advance algorithm like Hashed, AES, etc.
- Designing secured door lock to prevent unwanted access in the server room
- To give the user hassle free access without compromising security
- This system gives notifications about access to user

IV. PROPOSED SYSTEM

The proposed system has wide range of applications and can be used for various types of locks and systems, such as lockers, bicycles, cars, etc. Smart-Lock-System is a complete reinvention of the standard Key-Door lock, where all the digital keys are stored in a Digital Keychain kept on the owner's phone. Encrypted and secured Smart-Lock-System can be connected to the Internet via internet cable (UTP) or wirelessly (Wi-Fi).

In proposed system, divert the communication channel into Infrared signal that is outside of RF and gives a good range of mobility (eg. 15 - 20 meters) for SDL applications. We propose an infrared optical wireless unlocking for SDL with strong security mechanisms. We have designed and prototyped an Arduino and

Raspberry Pi 2 powered SDL system named Opt-Lock, and developed an accompanying Android smartphone application. An OptLock hardware accepts an infrared optical wireless signal (OWS) which contains the encodedkey via its on-board infrared (IR) sensor to unlock. This OWS is transmitted by the user through a smartphone via its on-board IR light emitting diode (LED). In the absence of an on-board IR LED, an external dongle containing an IR LED can be easily connected to the smartphone.1 IR OWS enables energy-efficient, directional communication with appropriate ranges for mobility, where visible light operates 1We also designed IR dongle that is powered through the smartphones 3.5 mm headphone jack for smartphones without IR emitter. with strict line-of-sight communication that inconveniences SDL type of applications. The encoding rate we developed using IR is (˜1.33k bps on average) is sufficient enough for\ applications like OptLock that needs to send a 128 bits long key in under a second. A detailed comparison of the various characteristics of the different communication mechanisms is illustrated in Table I. Our extensive experiments show 100% accuracy with 1.33 kbps average data rate can be achieved up to 20 meters of distance between a smartphone and a lock. It allows convenient remote access, easy access control and sharing as well as high security. Our experiments and analysis validate that OptLock offers a fast and efficient unlocking experience which is highly secure, and successfully thwarts various attack scenarios. OptLock offers the physical security of traditional door locks without the need to carry extra keys. The one-time-password scheme enables better security over existing smart locks along with easy key sharing among users. Our system overview is illustrated in the Figure 1. Users log in to our OptLock app by using their username and password. The username and password is then verified with a cloud server. After authentication with a cloud server, our application requests user ID, lock Access ID and public key from a cloud server. A server will send these details to the phone, which in turn transmits the authentication message to the lock. After receiving the authentication message, lock sends the user ID and lock Access ID to server. Server replies whether that user have access to lock or not. Now phone can send the authorization message, which can open the door.

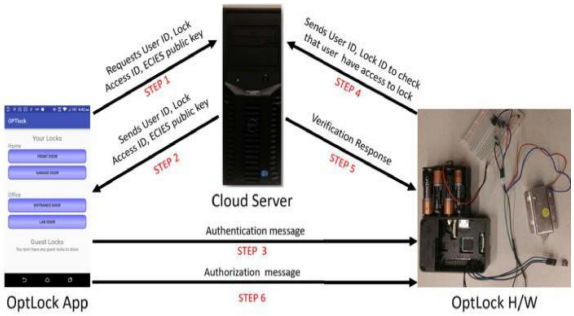

Fig. 1: - Opt Lock system overview

V. Hardware of Node

Hardware on the node includes Arduino, processor, Bluetooth modules and mobiles. The Bluetooth module is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Range is approximately 10 Meters (30 feet).

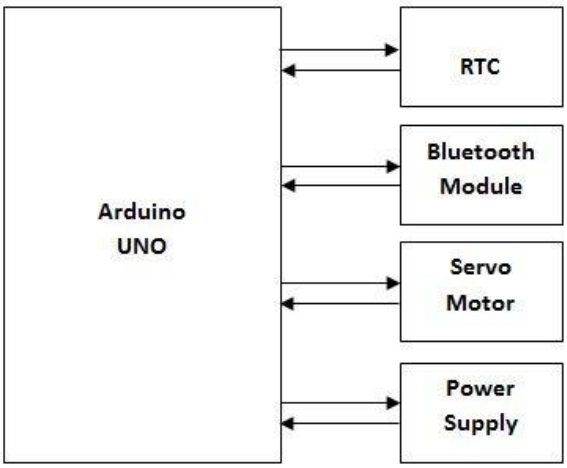

Fig. 2: - Block diagram

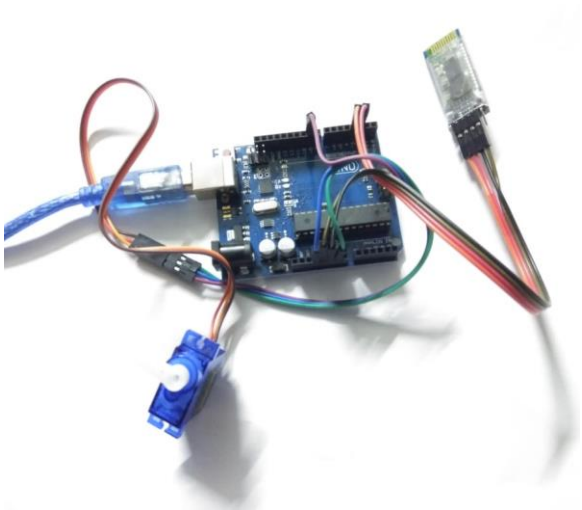

Fig. 3: - Hardware node

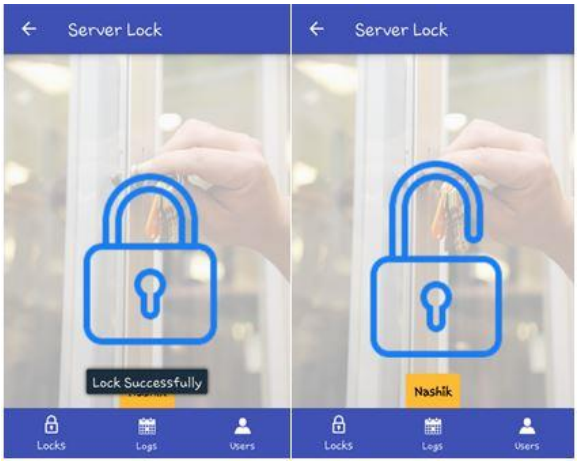

Fig. 4: - Result node

VI. OPERATING SCENARIO AND THE NODE AND NETWORK

Architecture:

Servo motors use feedback to determine the position of the shaft, you can control that position very precisely. As a result, servo motors are used to control the position of objects, rotate objects.

When user clicks on unlock button then servo motor rotate at 90 degree which will indicates unlock the door.

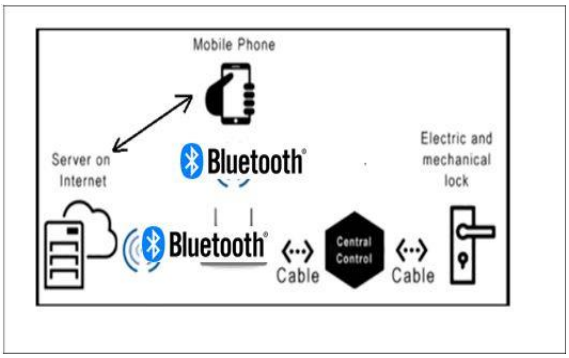

Fig. 5: - Architecture

VII. SYSTEM TESTS AND RESULTS

a) Hardware Testing:

While the data transmission system has been tested at our computer lab at nashik, the overall system node architecture has also been tested in computer lab in nashik city so as to ease all the test procedures. Regarding the communication channel, the data transmission was tested with the firebase as we are using Bluetooth module thus it is secured.

b) Software Testing:

Additional Diagnostics and debugging of the Arduino codes are done by Proteus tool and good results are achieved. Efficiency and the flexibility of the Arduino programs is also checked using proteus. The codes are error free and run efficiently on boards at real time. Real time simulations are also one of our systems before its implementation and good results are achieved.

VIII. RESULT ANALYSIS

Server Lock app is maintains lock and unlocks system. Servo motor gets rotate 90 degree when unlock button click. Firebase database add and control the lock logs system. All lock logs are maintained by firebase database. Bluetooth module is active when app gets open.

IX. CONCLUSION AND FUTURE SCOPE

Conclusion:

The Smart-Lock-System will open the door leading to a wide range of innovations in the world of lock systems wherever they may be. With its ease of installation and use, minimum complexity, wide applicability options, and strong feasibility, SLS guarantees a huge aspiring step forward into a better future lock system. All of the above can't be considered authentic on even possible without considerately taking into account one of the most vital aspects to the innovation: security. Therefore, after examining the detailed evaluation and explanation of this phase, the project really tackles the security concerns to eliminate any worries which might cause a threat to the systems success and prosperity.

Future Scope:

- There is a wide range of applicability to this system, not only be applied on home front doors, but as soon gates, cars, resorts with many locked areas and so on.
- Since system is a standalone system that operates by itself without the need for many requirements, and takes advantage of the power of mobile application and 3G networks to contact the server, system can also be used on car system with minimum infrastructure.
- Furthermore, system can be applicable on large buildings and resorts with many doors and each door for a specific set of users, and all these users share a unique key for the main gate.
- It can also be used in corporate once where not everyone has access to every department.

REFERENCES

[1] Qing ping Chi, Hairong Yan, Chuan Zhang, Zhibo Pang, and Li Da Xu, "A Reconfigurable Smart Sensor Interface for Industrial WSN in IoT Environment ", *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp.1417-1425, May 2014.

[2] M. T. Lazarescu,"Design of a WSN platform for long-term environmental monitoring for IoT applications *", IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, No. 1, pp. 45- 55,March 2013.

[3] F.Salvadori et.al., "Monitoring in industrial system using wireless sensor network with dynamic power management ", *IEEE Transactions on Instrumentation and Measurement*, vol. 58, no. 9, pp. 3104-3111, September 2009.

[4] S. Li, L. Da Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things ", *IEEE Transaction on Industrial Informatics*, vol. 9, no. 4, pp. 2177-2186, Nov. 2013.

[5] L. Wang, L. D. Xu, Z. Bi, and Y. Xu, "Data cleaning for RFID and WSN integration", *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 408-418, February 2014.

[6] ShrutiSridharan, "Water Quality Monitoring System Using Wireless Sensor Network" - International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 3, Issue 4, April 2014

[7] R.Karthik Kumar, M.Chandra Mohan, S.Vengateshapandiyan, M.Mathan Kumar, R.Eswaran, " Solar based advanced water quality monitoring system using wireless sensor network " - International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014 ISSN: 2278 – 7798

[8] Daudi S. Simbeye and Shi Feng Yang , "Water Quality Monitoring and Control for Aquaculture Based on Wireless Sensor Networks" - JOURNAL OF NETWORKS, VOL. 9, NO. 4, APRIL 2014

Web References:

[1] Shailaja. M. GundaNikkam, "Water Parameter Analysis for Industrial Application using IoT", IEEE 2nd IInternational Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)), pp.703 - 707, July 2016.