International Journal of Research in Engineering, Science and Management
Volume-2, Issue-2, February-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Survey on Smart Employee Locker System

Reshma Khalkar[1], Vaibhav Kadbhane[2], Punam Gite[3], Arti Darekar[4]
[1,2,3,4]*Student, Dept. of Computer Engg., Matoshri College of Engineering and Research Centre, Nashik, India*

***Abstract*: Nowadays, lockers are being used in all types of applications, from schools, universities to commercial businesses and more. That's why now, lockers can do more than ever before. There is a perfect storage solution for any application with digital and keyless lockers, specialized lockers, and even heavy duty lockers. Lockers are useful for all employees or facility users without needing to spend valuable time manually managing keys .Nowadays most of all are using a lock with providing key, by providing card which is used for swap or the authority can be given to open locker using biometrics like thumb. But today's company's requirement is that, they don't want to use all these things and they want to make their company smart. So by considering these requirements, the proposed system is for developing a digital locker system which user can open from his smart phone. In this system an android application is going to be developed by which user will manage the locker. The system will be based on Internet of Things. This system will be useful where strong security and digitization is required. This system is easily accessible by smart phone as now a days smart phones are used in daily life. It is user friendly. This system brings user more close towards the technology and automation and provides the security. At the same time this system is also affordable.**

***Keywords*: Bluetooth, Digital Lockers, IoT (Internet of Things), Raspberry-pi, Smart Locks.**

1. Introduction

Smart lock systems are installed in houses, cars, lockers and boxes for postal applications, logistic solutions, storage, etc. The lock can be opened by an electronic signal sent by a user close to it who wears a physical key (key fob, card, smartphone, etc.) conveniently authenticated by a secret digital key. The digital keys are obtained from a web app, in the case of smartphones, generated from a key exchange cryptographic protocol or directly stored in the memory of the physical key. Digital keys should be employed with high security to ensure that unauthorized users cannot open the lock nor do a malicious use of them. Several smart lock systems available in the market are based on Bluetooth, which is a wireless communication standard that connects devices via short-range radio. Many types of services and profiles have been defined to use Bluetooth in a wide area of applications that range from devices that provide information, such as the physical key, to devices that accept commands, such as the lock (in the case of a smart lock system). Besides, since this technology can connect anything to Internet, it has gained a great attention in the context of Internet of Things. Bluetooth LE (BLE) and Bluetooth BR/EDR (basic rate/enhanced data rate) are the two forms of Bluetooth wireless technology systems most common today. The first one, which enables products that require lower current consumption, lower complexity and lower cost than BR/EDR, is the one usually employed in smart lock systems. The Bluetooth security model includes five features: (a) pairing (the process for creating one or more shared secret keys), (b) bonding: the act of storing the keys created during pairing for use in subsequent connections, (c) device authentication (verification that the two devices have the same keys), (d) encryption (which ensures message confidentiality), and (e) message integrity (to protect against message falsifications). Security is always based on the secrecy of the shared digital keys. However, digital keys can be revealed with passive eavesdropping attacks that can be done at pairing or with physical attacks directed at reading the non-volatile memory of the physical key. If non-volatile memories are not protected, they can be revealed not only through simply reading them but also using more elaborated techniques, such as optical probing with a laser and electromagnetic analysis. Since a non-volatile memory retains information even removed from the device, the attacker can have multiple opportunities and ways of retrieving the digital key and make a copy of the physical key. The lock could be opened by an attacker and the legitimate user could not realize that. The solution proposed in this paper is more secure because the secret digital keys never go out the physical keys and are never stored. They are generated when required and removed later. This is possible thanks to the use of the start-up values of the SRAM in the BLE chip of the physical key. If SRAM cells are powered but not written, the positive feedback between the two cross-coupled inverters that form a cell leads it to the start-up value imposed by the inverter which begins to conduct. The conditions that make one inverter be the winner are related to mismatching between the inverters, which are usually due to unique and random fabrication process variability of each SRAM.

2. Literature survey

M.A. Prada Delgado [1] develop Bank Locker Security System based on RFID & GSM technology in which system can authenticate, validate the user & unlock the door in the real time for bank secure access. It was very time consuming system. Gaurav Chavan [2] has developed physical unlockable keys for smart lock systems using BLE. The BLE is used for communication establishment between physical key and locker. Also SRAM is used. Depending on the start u values of SRAM secret cryptographic keys are reconstructed. This system is

cheaper. Airing process in this system is not secure. Grant Ho Derek [3] had developed Bank Locker security system using Android Application with the help of Bluetooth, Android Application and OTP is sent to users hone. It has three level security and it inform user when locker is opened via SMS. But if users hone is stolen then it is harmful for user. Prof. R. Shrinivasan [4] developed Advanced Locker Security system which uses technologies like RFID, GSM. In this system password verification is done. This system provides security and reduces the waiting time of consumer. But the system is expensive.

3. Methodology

There will be three modules in the system as follows:

- *Android app to control locker:* This will be the front end module or the GUI of the system. Here the user will give the input to unlock the lock by his cell phone. The signals will be generated through the BLE and will be given to the microcontroller.
- *Communicate locker with android app using BLE:* The microcontroller will receive the send command. Also the information will be stored in the database.
- *Control actual lock:* Here actual lock will be open by actuators. This System is mainly designs for employee's .In case if user is far away from the locker and in case of emergency he will be able to open the locker remotely. For example if the employee is at home and there is requirement of file in industry then he could access his locker from remote location. The block diagram for the system is given below

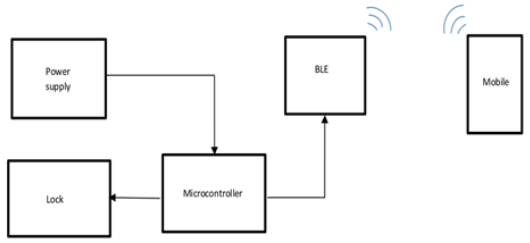

Fig. 1. Block diagram

4. The BLE module

Bluetooth Low Energy (BLE) is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group (Bluetooth SIG) aimed at novel applications in the healthcare, fitness, beacons, security, and home entertainment industries. Compared to Classic Bluetooth, Bluetooth Low Energy is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range. Mobile operating systems including iOS, Android, Windows Phone and BlackBerry, as well as macOS, Linux, Windows 8 and Windows 10, natively support Bluetooth Low Energy. The Bluetooth SIG predicts that by 2018 more than 90% of Bluetooth-enabled smartphones will support Bluetooth Low Energy [8].

5. Conclusion

Lockers are very useful in various field like industries, banking sectors etc. This paper work has been carried out for providing a strong security. Also digitization is added to the traditional locker systems using proposed system. The system is more user friendly and cheaper. In case of cell problem user can contact to admin and can stop his service temporarily.

Acknowledgement

We express our sincere thanks to all those who have provided us valuable guidance towards the completion of this paper. We hereby take this opportunity to record our sincere thanks and heartily gratitude to Prof. A. V. Dighe mam for her useful guidance and making available to us her intimate knowledge and experience for this project.

References

[1] Gaurav Chava, Sourabh Dabke, Anup Ghandghe, and K. A. Musale, "Bank Locker Security System Using Android Application," in International Research Journal of Engineering and Technology, vol. 2, no. 1, April 2015.
[2] R. Srinivasan, T. Mettilda, D. Surendran, K. Gobinath, and P. Sathish Kumar, "Advanced Locker Security System," in International Journal of Advance Research in Science and Engineering, vol. 4, Special Issue 1, March 2015.
[3] R. Ramani. S. Selvaraju, S. Valarmathy, and P. Niranjan, "Bank Locker Security System based on RFID and GSM Technology," in International Journal of Computer Applications, vol. 57, no. 18, November 2012.
[4] Grant Ho Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song and David Wagner, "Smart Locks: Lessons for Securing Commodity Internet of Things Devices," ASIA CCS '16 May 30-June 03, 2016,
[5] T. Denning and T. Kohno, "Empowering consumer electronic security and privacy choices: Navigating the modern home," in Symposium on Usable Privacy and Security (SOUPS), 2013.
[6] S. Drimer and S. J. Murdoch. Keep your enemies close: Distance bounding against smartcard relay attacks. In USENIX Security, 2007.
[7] Danalock. http://www.danalock.com/