ISSN No:-2456-216

Smart Unlock System for Home Invasion Protection

Nisha Mary Philip
Department of Electronics
Toc H Institute of Science and Technology
Kerala, India

Dr. Gnana Sheela K
Department of Electronics
Toc H Institute of Science and Technology
Kerala, India

Abstract:- In single households, crime and dacoity is increasing at an alarming pace and poses a new concern for the local authorities. Most single female families and households are also faced with the consistent anxiety about strange visitors and stranger invasion. This paper speaks about an OTP-based door-lock system has been proposed that provides enhanced security of digital door-locks while curtailing the problems associated with the current digital security systems. The system describes an efficient and effective design of a door-lock equipped with special features such as OTP based system for password generation following visitor arrival and visual confirmation by the resident whether the visitor is familiar or not, thus preventing forced break-open.

Keywords:- *Burglary; Break-through; Dacoity; Image capture; OTP generation; Visual confirmation;*

I. INTRODUCTION

Burglary refers to the crime of entering a building or any area illegally in order to steal. FBI reports over many years states that 58.3% of all the burglaries, theft and crimes in the world involve forceful entry into premises. The most recent statistics speaks out that, a burglary takes about 90 seconds to a maximum of 12 minutes for completion, and considering an average timing, a burglar will break into a home or residential premises within a span of 60 seconds. Most burglars and people, who plan to break in, target cash first followed by other expensive items like jewelry.

Primarily, any home security system aims to protect the life and property of those residing inside it from burglary, robbery etc. The security concerns in an area where people resides, is a situation that needs careful assessment. It is of paramount importance that proper measures are in place which will address the safety and security concerns in the area. Security, by definition, is the freedom from, or resilience against, potential harm caused by others [3]. Reframing the definition, security involves those things that you do to protect somebody/something from attack, danger, thieves, etc. With the escalating number of single households, constant acquaintance with crime and dacoity are emerging as a new social problem. Significantly, in the case of female oriented families, consistent tension and worries of stranger visitors also exists alongside. Most people are in the constant search of systems which can ensure protection to the core for their residential premises, workplaces etc. Shocking are the existing statistics, but the good news is that there are several preventative measures that one can take to burglar-proof their home and protect their loved ones. The present project will serve this purpose to the fullest and employs an OTP-based door-lock system that augments the security of many prevailing digital door-locks [4]. The system consists of a door-lock with many efficient features such as use of OTP password, image storage and a web view with features comprising real-time image captured monitoring, door lock control and event logging.

II. LITERATURE SURVEY

Residential theft is a common problem that we face as a society and normally occurs when the property is vacant. A census of violence resulting in serious injury or even death is rare. Most commonly, theft at households and offices involve household staff or office staff either stealing directly from their employer or allowing acquaintances to strangers into the residence while the employer is away. According to another study, a burglary takes place every 3 minutes and the time is up that we reconsider the safety standards of our homes. Burglaries and thefts continue to destroy and severely impact every country including ours.

As per the National Crime Records Bureau (NCRB) reports, 2, 44,119 cases of theft, burglary etc. took place in many residential premises and societies in 2017. In the year 2016 the number of such cases stood at 2, 20,854, which was a huge leap of over 10%.

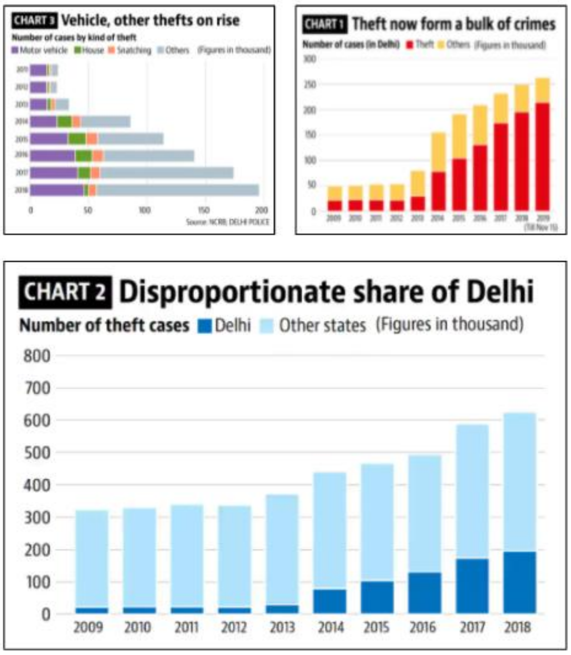


Fig 1: Various crimes and their shocking rates in our country.

In 2017, the value of property stolen and robbed from residential premises was Rs. 2065 crores, which is a 40% increase from Rs. 1,475 crores stolen in the previous year 2016. Figure 1 and 2 illustrate the scenarios in detail. On

November 15, 2020, which marked the first anniversary of the company Godrej, #HarGharSurakshit initiative was celebrated. Godrej Locks launched and kick-started a 'Free home safety assessment program' to encourage them to take precautionary and protective measures against burglary.

Cyber criminals have been found to use innovative and modern tools and tactics and hence security and alert teams must respond to it likewise. A lot of information is available in literature on this social issue [1].

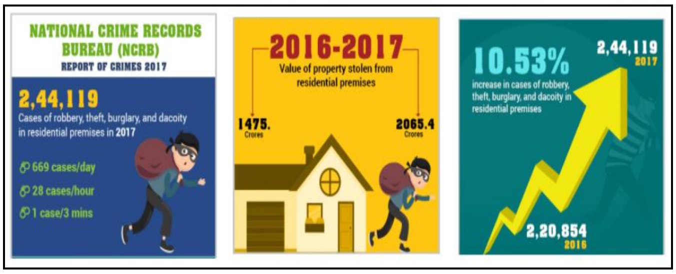

NATIONAL CRIME RECORDS BUREAU (NCRB)
REPORT OF CRIMES 2017
2,44,119
Cases of robbery, theft, burglary, and dacoity in residential premises in 2017
669 cases/day
28 cases/hour
1 case/3 mins
2016-2017
Value of property stolen from residential premises
1475. Crores
2065.4 Crores
10.53%
increase in cases of robbery, theft, burglary, and dacoity in residential premises
2,44,119
2017
2,20,854
2016

Fig 2: Census showing the crime rates in different part of the country

The manuscript entitled 'Theft Detection System using PIR Sensor' (2018) describes a novel method to prevent theft. PIR sensor is, by definition, a motion detector which is used to sense the heat emitted by a living organism and integrating it with Raspberry Pi. But the major disadvantage of PIR was that it is easily hindered by other sources of heat and moreover, the sensing effect can be influenced by RF radiation as well. When the temperature measured is close to the human body temperature, the detection and sensitivity will reduce, and sometimes even short-term failures also occur. Due to these inherent deficiencies, the method failed to catch the eye of the customers.

In 2010, the design and implementation of an Embedded Home Surveillance System using Multiple Ultrasonic Sensors was published wherein ultrasonic sensors were used to counter burglary. But this method failed miserably as ultrasonic sensors were highly sensitive to variations in ambient temperature. Smart Digital Door Lock for Home Automation (2009) utilizes digital locks where a specific password is used to lock and unlock. In most safety systems, passwords are preferred for reasons of price and convenience [7]. However, it is imperative to take an extra ounce of caution not to leak the password, and it is highly recommended that the password be changed frequently, but it is not often feasible. Further, the password of a door lock can be decoded and leaked by the use of UV light or hidden cameras.

According to a recent study, almost 83% of the people change their password every 6 months. The data also revealed that almost 30% of the thefts in India are digital thefts, which is quiet shocking [1]. Most of the current security systems have been rejected by users due to multiple disadvantages. For example, in the case of keypad systems, we need to type in a unique password or numeric code to open or close a door. Curiously enough, there are so many different codes and passwords that we need to memorize in our daily lives to access various apps, email etc. In addition we're always told to pick a unique code for each system in order to heighten security, but there is a limit to the human mind's capacity [8]. Adding another code for unlocking our doors can sometimes prove frustrating especially when the code has been forgotten. Since the same keys are used time and again to input the same password, those numbers or letters can get wiped off reducing the appeal of the keypad. The password, if used repeatedly, can get into wrong hands. This means that if the password for one service gets into the hands of an unauthorized person, he can get access to that particular service [9].

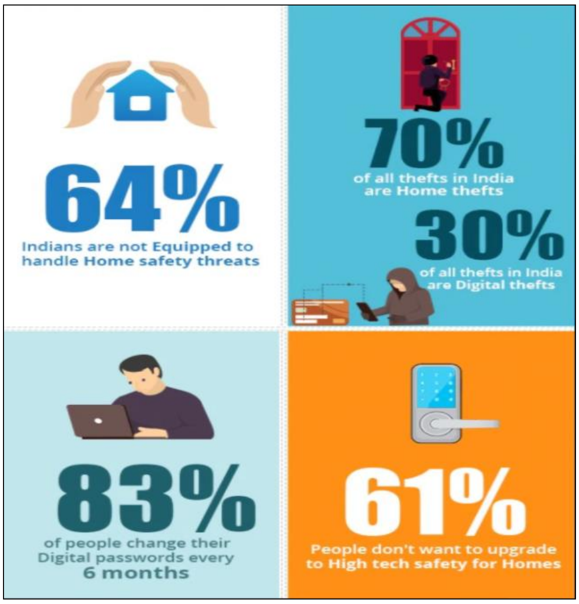

64%
Indians are not Equipped to handle Home safety threats
70%
of all thefts in India are Home thefts
30%
of all thefts in India are Digital thefts
83%
of people change their Digital passwords every 6 months
61%
People don't want to upgrade to High tech safety for Homes

Fig 3: Shocking numbers revealing the percentage of digital thefts

Conversely, a system becomes more efficient if a new password is generated every time and the password cannot be leaked to another individual.

III. OBJECTIVES

The proposed system has been so designed to work as a solution against all the prevailing safety systems that suffered huge setbacks due to inherent flaws. It is an OTP-based door-lock system that accords protection against burglary, theft, dacoity etc. through effective visitor identification and verification prior to his entry.

IV. METHODOLOGY FOR THE PROPOSED SYSTEM

The present study veers around development of an OTP (One Time Password) based technology to prevent forced break-in, relieving anxiety of the residents from unfamiliar visitors. The process is set in motion when a person rings the doorbell. Once the bell has rung, the resident gets to know that someone is at the doorstep. The camera module set in front of the door immediately captures the image of the visitor. The captured image is then sent to the resident and stored in the database. The resident then checks the image and he/she can easily figure out whether the person at the doorstep is familiar or not. Following confirmation of the identity of the individual, the OTP generation system can be guided to create an OTP. If the person is an unknown individual, then nothing is done further. However, if the person at the doorstep is a familiar individual, then the resident clicks on the generate OTP button and the OTP is generated and becomes visible to the resident. The resident then sends the OTP to the visitor. The visitor after receiving the OTP enters the OTP using the keypad in the doorbell system. The system then performs OTP synchronization using the OTP entered by the visitor and that generated by the system. If the synchronization process is complete, then the door unlocks.

However, if the synchronization fails more than 3 times, either a break-in notification is sent to the resident or nothing further is done and the door remains closed. If a break-in notification is sent, the resident then initiates the break-in mechanism i.e. call an emergency number or ring an alarm.

Thus this mechanism ensures a very efficient means to prevent the break-in that can happen in places like residential premises or homes, offices etc.

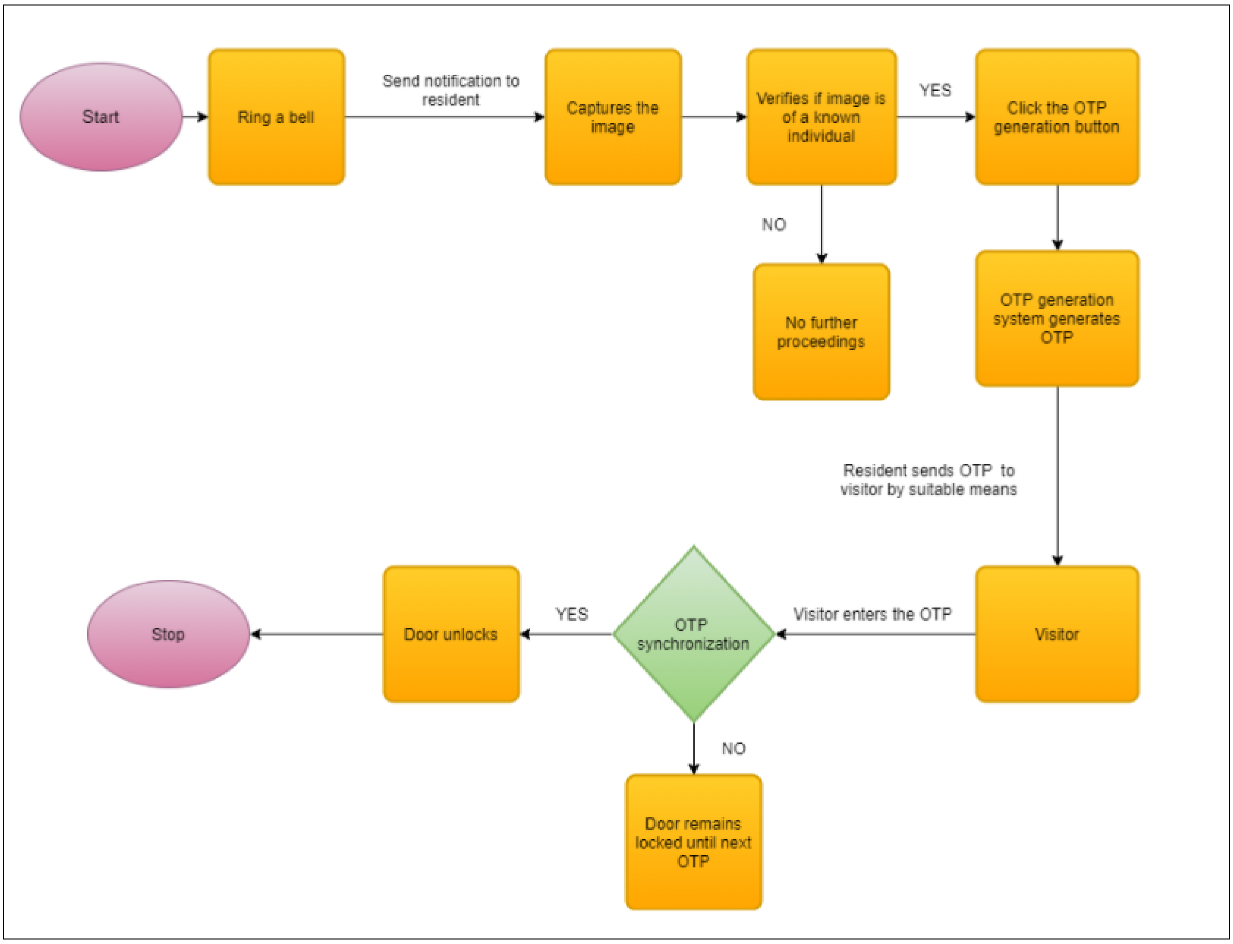

Start
Ring a bell
Send notification to resident
Captures the image
Verifies if image is of a known individual
YES
Click the OTP generation button
NO
No further proceedings
OTP generation system generates OTP
Resident sends OTP to visitor by suitable means
Visitor
Visitor enters the OTP
OTP synchronization
YES
Door unlocks
Stop
NO
Door remains locked until next OTP

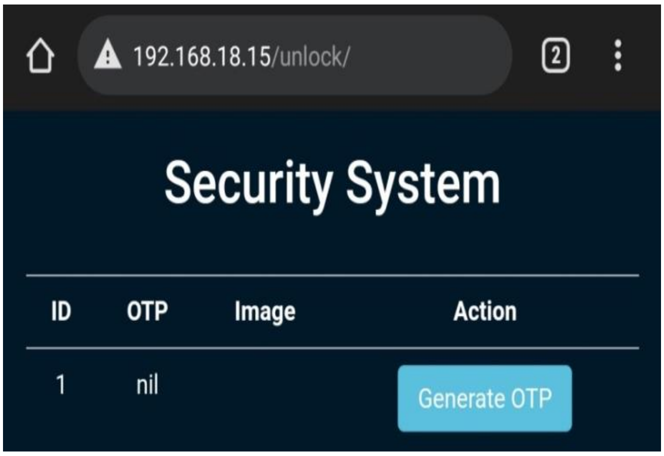
Fig 4: Flow diagram of the methodology implemented.

A Code Flow

```
                         Switch press (Arduino)
                                   |
                      Inform python of switch press
                                   |
Camera image capture and save image to XAMPP/htdocs/profolder/images/datetime.jpg
                                   |
                     Check if OTP button clicked or not
                                   |
                              Generate OTP
                                   |
                      Goto OTP mode and type OTP
                                   |
                           Pass OTP to python
                                   |
                  Check and see with the generated OTP
                       |                          |
                   If correct                 If wrong
                       |                          |
                   Relay open        If count is not 3, next try for OTP
                                |
                         Clear image and
                           OTP at db
```

V. RESULTS AND DISCUSSION

The entire process starts with a person ringing the bell. The initial steps in Arduino and python code involve the initialization of the different pins and declaration of the variables which are used during the entire procedure. These variables once declared can be used throughout the entire program to store some values during implementation and to perform specific actions using these variables.



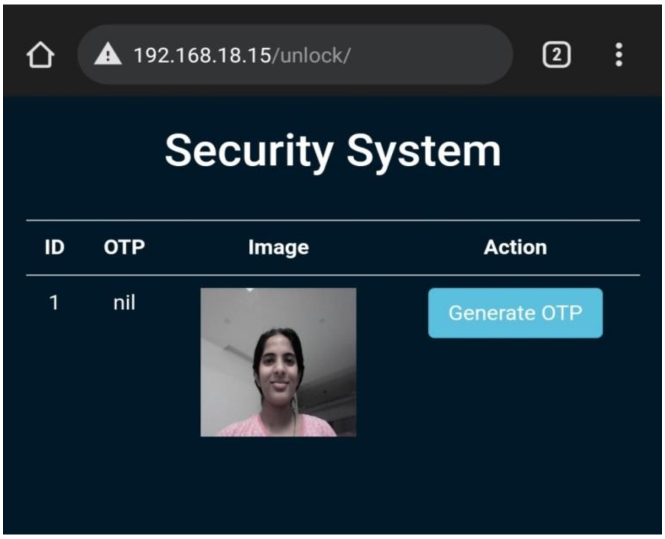
192.168.18.15/unlock/

Security System

ID	OTP	Image	Action
1	nil		Generate OTP

Fig 5: Web view of the security system implementation

The LCD screen will initially display 'Security System' when no functionality has been performed. When the bell has rung, the Arduino informs python that the bell has been pressed indicating the presence of an individual at the doorstep. Before a person waiting outside needs to enter a premise, verification of the identity of the visitor has to be completed and the most ideal method would be to perform a visual identification.



192.168.18.15/unlock/

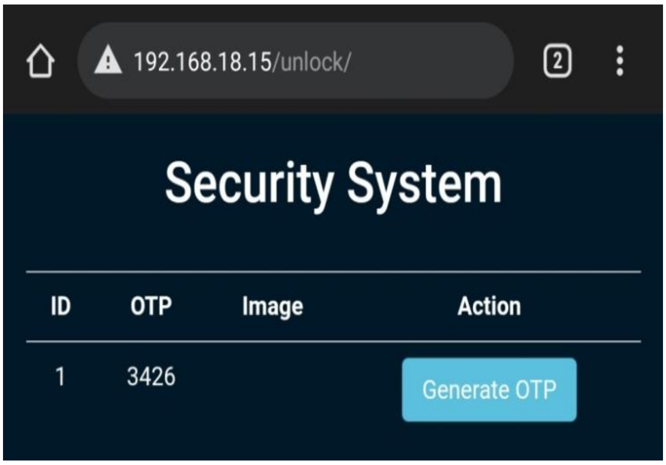
Security System

ID	OTP	Image	Action
1	nil		Generate OTP

Fig 6: Web view layout when the image has been captured

The image of the visitor is now captured by the system. When the bell is rung, the switch is made to a LOW state and Arduino sends a 'Capture' message to python.

Python code is executed and the image of the individual is captured. It is imperative that we wait for about 50 frames of the image to be developed by the system before the image is captured. This ensures that the image captured is not blurred and inappropriate and the correct visual identification of the visitor can be made by the member of the household. The captured image is then stored in a predefined location and 'Image Write' message will be displayed on the python run window during the image capturing procedure.



Security System

ID	OTP	Image	Action
1	3426		Generate OTP

Fig 7: Web view layout when OTP is generated

When the bell is rung, the LCD display reads 'Calling Bell'. The platform where the OTP generated and the picture captured is displayed has been developed as a web view. The captured image is verified by the household and if the visitor is a known person, then click 'Generate OTP' button. This leads to switching the mode to OTP mode and the image captured is erased. After a 5 sec delay an OTP is generated under the OTP heading. The LCD screen now reads 'Enter OTP'. The OTP generated and displayed on the table can be entered using the keypad/ keyboard module. The module also permits deletion of digits if entered erroneously, and once the OTP has been entered correctly, then press the ENTER key. This results in the OTP being fed into the system and the synchronisation procedure is triggered. While synchronisation is in progress, the LCD screen reads 'Validating OTP '.

The python performs string equality checking to ensure whether the entered value using keypad and that generated by the system is exactly the same. If the 2 strings match, then the relay switch which was initially set to a value as LOW is then turned to a HIGH state which is used to symbolize the door which will then unlock. The LCD screen will now display 'OTP Entered is Correct' and the relay switch will be high indicated by the LED which will remain lit up until the time the relay switch is in the high state. The LED will stay lit up for a period of 5 sec and the LCD will read 'Door closes in (time) secs'.

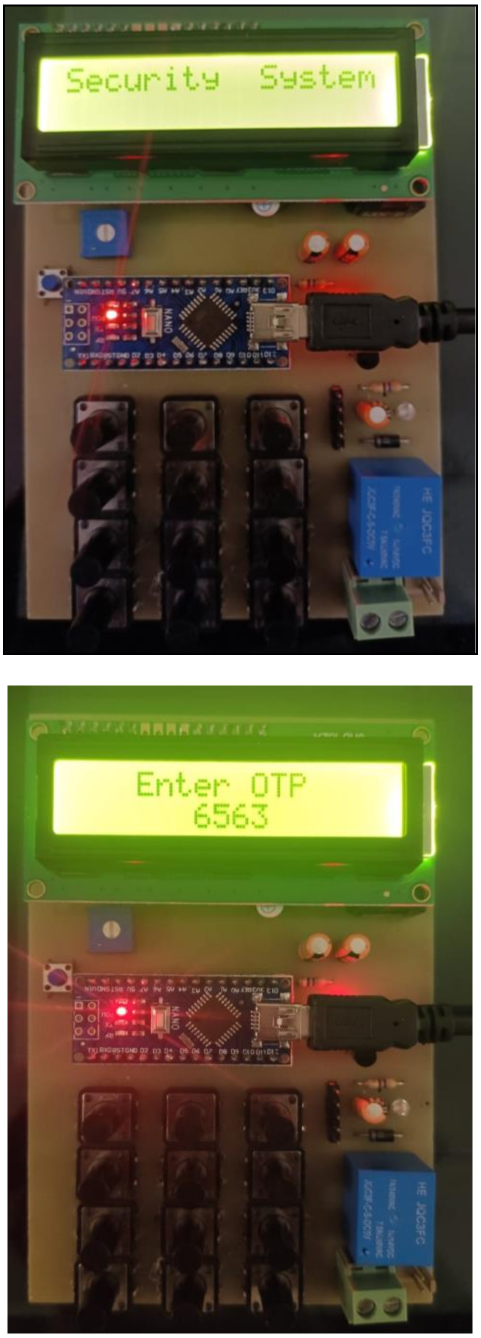


Fig 8: LCD display during start and when OTP is entered

The time parameter will display numbers from 5 to 1 in the decreasing order to show the count down after which the door will lock again. To unlock the door, the visitor has to repeat the same procedure once again, with the LCD screen displaying 'Security System'.

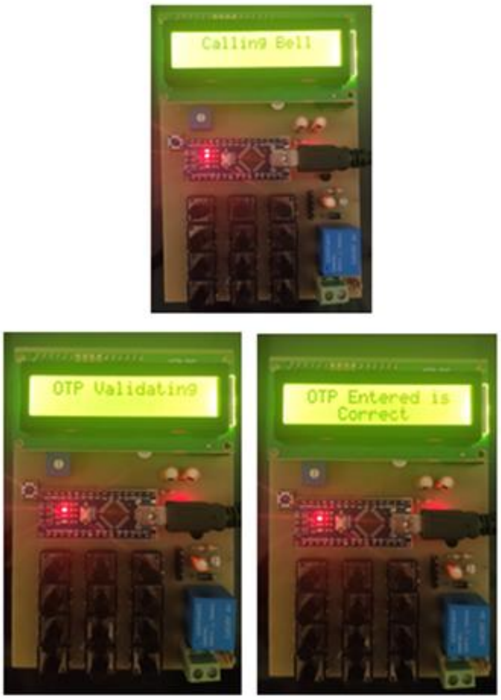


Fig 9: LCD display during ringing the bell, when OTP entered is validated and when OTP entered is correct

The next scenario to be evaluated is when entered does not match with the generated OTP. If, however, the entered OTP does not match with the system generated OTP, the system performs a synchronisation procedure and finds that it is a mismatch.

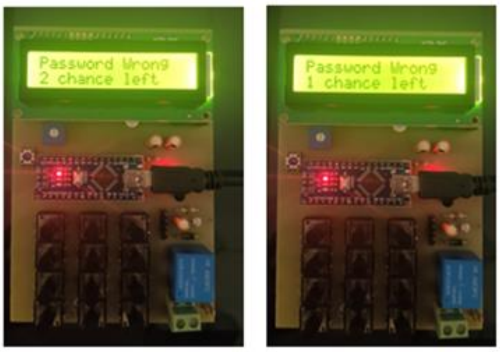


Fig 10: When password mismatch occurs, and when only 2 and 1 chance is left.

When a mismatch occurs, the LCD shows a display stating that the value entered is a wrong entry and also displays the number of attempts left to retry.

The procedure can be repeated for 3 times after which the display states that all the attempts have completed and the door will remain locked.

Further, the current OTP is also erased from the system memory. Now to open the door, the visitor has to repeat the entire procedure from the beginning by ringing the bell to notify his/her presence at the doorstep.

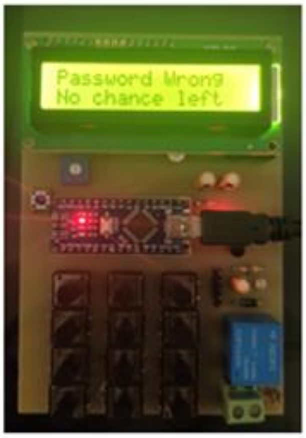


Fig 11: When password mismatch occurs, and when no chance is left.

VI. CONCLUSION

The proposed system provides an efficient means to overcome the issue of burglary and anxiety to the user. Since it is an OTP based system, the disadvantages associated with the conventional method of using the same numeric or word password for gaining access to the inner premises, are overcome Another advantage is that the resident has the complete control of deciding whether or not to grant permission to the visitor to enter the house. The fear of a password getting leaked or falling into the hands of unauthorized persons are also avoided as each time a new OTP is generated while the old one gets erased immediately from the system memory .

This system further allows single-person residents to be relieved of their tensions due to password leakage, unforeseen visitors etc. thus addressing their concerns. The proposed system further has to be installed in households and has to be compared with various existing ones, so as to assess the effectiveness of the novel system regarding convenience to the user.

VII. FUTURE SCOPE

The system is currently designed as a web view where no specific notifications and alert messages will be received by the user when a visitor rings the bell. But in practice, this is expected. Thus, when a visitor rings the bell, a notification must immediately be forwarded to the resident so that he can initiate further proceedings leading to OTP generation. Android programming developments can be incorporated into this application to transform the web view as an app wherein immediate notifications will be received by the resident following the arrival of a guest.

REFERENCES

[1.] Joongjin Kook, Design and Implementation of a OTP-based IoT Digital Door-lock System and Applications, IJERT, 2019, Volume 12, Number 11.

[2.] Hee Kyung, S., “The analysis of Solo Economy,” 2017 Research Report part 2, Statistics Korea, 2017, pp. 153-173.

[3.] Wei-Jun, J. Y., Adam, K. C., "Living alone: One person households in Asia," Demographic Research, 32(40), 2015, pp. 1099-1112.

[4.] Report of the Single-person household of South Korea 2018, KB Financial Group Inc.

[5.] Mr. Patil Bhushan S, Mr. Mahajan Vishal A, Mr. Suryawanshi Sagar A, Mr. Pawar Mayur B, Prof. Mr. U. R. Patole, "Automatic Door Lock System using PIN on Android phone", IRJET, 2018, Issue: 11

[6.] Anti-spying Kit for a Digital Door-lock, http://news1.kr/articles/?2782470.

[7.] Jeehyun, K., "Korean Crime Victimization Survey," Korean Criminological Review, 28(2), 2017, pp. 287-320.

[8.] Daegyu, S., Hanshin, G., Yongdeok, N., Design and Implementation of Digital Door Lock by IoT, KIISE Transactions on Computing Practices, 21(3), 2015, pp. 215-222.

[9.] Samsung SDS SHP-DR900, https://smarthome.samsungsds.com/doorlock/product/view?prdId=137&searchWord=&searchPrdType=SD&searchCateId1=4&searchCateId2=0&locale=ko

[10.] Edoardo Persichetti,"Secure and Anonymous Hybrid Encryption from Coding Theory", Springer-Verlag Berlin Heidelberg 2013.

[11.] Kaustubh Dhondge Kaushik Ayinala Baek-Young Choi Sejun Song, "Infrared Optical Wireless Communication for Smart Door Locks Using Smart phones", 12th International Conference on Mobile Ad-Hoc and Sensor Networks, 2016.

[12.] B. Rhodes, "Designing an access control system", https://ipvm.com/reports/designing- an-access-control system", 2015.

[13.] Abdallah Kassem and Sami El Murr, "A Smart Lock System using Wi-Fi Security", 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA) 2016.

[14.] Wen-Chung Kao, Chil-Chao Wei. Automatic phonocardiography signal analysis for detection heart valve disorders. Expert Systems with Applications. 38 (6) (2011) 6458-6468.

[15.] V. Nivitha Varghees et al. A novel heart sound activity detection framework for automated heart sound analysis. Biomedical Signal Processing and Control. 13 (2014) 174-188.

[16.] SK Yoo, and HJ Kim, "The Policy and the Trend of Standardization for Internet of Things," Journal of KIISE, Vol. 28, No. 9, pp. 21-27, 2010.

[17.] M. Roland, "Software card emulation in nfc-enabled mobile phones: great advantage or security nightmare", in Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, 2012.