Grenze International Journal of Engineering and Technology, June Issue

Cost and Energy-Efficient Digital Code Lock for Smart Homes using Seven-Segment Displays in Verilog HDL

Pragati Agrawal[1] and Shobha Sharma[2]
[1-2]Indira Gandhi Delhi Technical University for Women, New Delhi, India
Email: pragati011mtvlsi20@igdtuw.ac.in, shobhaa_sharma16@yahoo.co.in,shobhasharma@igdtuw.ac.in

***Abstract*—The rationale behind smart homes is to provide a secure and comfortable life. The concept has gained attention in the last decade. Safety and security of smart homes is one of the most important challenges that have been addressed many times. In the trending era, it has been proven via several studies that the traditional lock-and-key system is no more effective in providing security to smart homes. This paper proposes designing a simple digital code lock to enhance security of smart homes. The system uses five 7-segment displays. If the entered passcode matches the authentic code, the user is given the access, else his/her access is denied.**

***Index Terms*— Smart home, Verilog, Security system, Door, Access.**

I. INTRODUCTION

Home automation comes up with safety and convenience by permitting the home occupants to control and monitor the appliances remotely. H. Hamzah et al. [1] proposed a design of a remote controller lighting system using slide switches that could control various LEDs. Smart homes add to the quality of life and promote independence in living standards. They are beneficial for persons of all age groups and for disabled persons as well. Smart homes can be modeled as an energy-efficient replacement for institutional care.

Security has become a serious issue for everyone. The advancements of technology have raised a huge demand for simple but strong security systems that can be easily installed in homes. Some studies have been made that agreed that smart homes are vulnerable to theft and robbery with traditional key-and-lock systems [2]. The biggest drawback of such old-style systems is duplication of the keys. Such weak security systems have proved to be inefficient in avoiding break-in [3,4]. This arouses the need of building a robust security system which can be monitored remotely.

This paper puts forward a digital code lock system for smart homes. The password-based lock systems are considered one of the most preferred choices due to their simplicity and cost-effectiveness. The design is implemented using Verilog HDL. This keyless security system allows only the house owner to unlock the door after entering the correct hexadecimal code in five 7-segment displays. The system will activate an alarm signal if three incorrect attempts have been made consecutively. The paper is divided into a number of sections briefing about the existing systems, the methodology adopted for system designing, simulation results and conclusions.

II. LITERATURE REVIEW

A. Existing Security Systems

M. Tseng et al. [5] proposed a design for door opening using a single wrist-worn sensor. Th e sensor is

Grenze ID: 01.GIJET.8.2.4

responsible for taking notes of movements of the upper limb of a person. Three sub-gestures namely grasping, rotating and opening the door, are identified by the sensor. The relevant data is collected in a datasheet for processing. It was observed that the system was 93.3% accurate and 89.6% precise in making the observations.

An Arduino based security system [6] was designed by Sriharsh B. S. et al. It prompts the user for a passcode to unlock the door. Arduino has the responsibility of reading the entered passcode. If correct code is entered, the door opens for a stipulated amount of time, else an error message is displayed on a 16×2 LCD unit and a beep sound is given out by a Piezo buzzer. The contrast of the LCD display is adjusted by a potentiometer. This system finds uses in bank lockers, doors and computers for BIOS locking among others only until the secret code is masked from others except the owner.

The product designed by Saleh et al. [7] uses push buttons of Altera DE2 Trainer Board to input user data for unlocking the doors. It also senses uneven motion and uncertain temperatures for enhancing security. The sensed data is transmitted to the FPGA as analog signals for processing. The results are displayed on 7-segment displays and LEDs.

Nasir et al. [8] implemented a keyless lock system on Altera DE2 Trainer Kit and simulated it on ModelSim software by Mentor Graphics. The passcode to unlock the door was created by the code and code length variable. The door is unlocked by entering the correct passcode using slide switches on FPGA. The system goes to deep-sleep mode after three consecutive failed attempts.

Yuan-Chih Yu [9] built the most practicable prototype which combined a smart card (carried key) and a touchscreen panel (non-carried key) to unlock the door. But the author suggested that the keypads and touchscreens are not much effective. So he used a virtual technology which unlocked the door by finger gestures. The prototype was aimed to provide a better living experience. In case of power failure, the system could survive by being connected to a mobile power bank via a USB port. A key hole was also provided for opening the lock traditional way in case of power failures. It was concluded that a non-carried key is a better option as smart cards can be lost due to several reasons.

Hitesh Prasad et al. [10] designed a digital (electronic) locker in Xilinx ISE and implemented it on the Artix7 DDR4 FPGA. The locker consisted of 3 phases-reset/change password, locked and unlocked phases. Upon entering the correct 4-digit key the system is unlocked. If the wrong code is entered, an error signal is prompted. If 2 subsequent keys are pressed in more than 10 seconds time, then the system produces a timed-out signal and will enter the timed-out state. Every time to come out from the timed-out state or pressed-wrong-key state, UnLk key needs to be pressed manually.

H. Alnabhi et al. [11] designed a security system that allows only the responsible person, i.e. the user, to get in the house. The system uses a fingerprint scanner, interfaced with Arduino microcontroller ATMEGA328P, to identify the authentic biometrics, and a password keypad for enhanced security. An LCD displays the instructions to be followed. A camera is incorporated to monitor whom the access has been given/denied. The security lock gives access only to the registered users and opens the door for five seconds. A record is maintained for those who have been given the access. In case any unregistered user tries to open the lock, the owner is immediately notified through an SMS sent via GSM technology.

Somjit Nath et al. [12] designed an Arduino based door unlocking system for intended application in Laboratories and libraries. The system used a central server to collect and store useful data. Each user was assigned a serial number burnt on their RFID tags and stored in a database on the server. Through RFID technology the access was made restricted to only authorized personnel. The communication between the server and the door took place via wireless transmitter and receiver. An option of manual operations via buttons was included for use in emergencies and intrusions. All the activities were being monitored through an online monitoring system.

K. Saroch et al. [13] implemented an automatic security system for machines or objects using FSM. It was designed in VHDL using Xilinx state CAD tool. The rationale behind the system was that it opens the lock only when it detects a particular sequence. If the wrong code is entered, the lock remains closed. The design is then verified on the FPGA SPARTAN3 board. The responses are obtained quickly with less power consumed.

S.Subba et al. [14] proposed a security system based on GSM technology. The system was designed in VHDL and implemented on the SPARTAN 3E board. The system prompts the user for an authentication code. Upon entering the correct code, GSM technology gets activated and sends an OTP on the user's mobile phone. The OTP pushed by the GSM technology expires in 3 minutes. Only after entering the OTP within 3 minutes and getting it verified by the system, the user is given access. If any of the entered code is wrong, the access is denied. All the instructions and results are displayed on a LCD screen of the FPGA board.

B. Verilog Hardware Description Language (HDL)

Verilog is a Hardware Description Language used for writing design formats for electronic circuits and systems. Its intended utility is to verify the logic and functionality of designs via timing waveforms. Writing Verilog scripts makes it easy for designing and debugging large circuits as compared to schematics. At present, Verilog HDL is one of the most popular and in demand HDL for digital circuits designing. A Verilog design comprises a ladder of modules which communicate among themselves via unidirectional and bidirectional in-out ports. Verilog HDL is indifferent from software programming languages in the way they provide information about time and signal sensitivities.

C. Xilinx Vivado Tool

Xilinx is the chief pioneer of complete programmable logic solutions together with advanced circuits and software design tools [13]. Vivado Simulator is a component of Vivado Design Suite, software built by Xilinx to simulate, synthesize and analyze HDL entries of digital circuits. It has been re-developed by Xilinx from scratch considering novel algorithms for various steps involved in physical designing. Collaborative design environments are facilitated to the designers for better productibility.

III. METHODS

Xilinx Vivado 2018.2 simulator software has been used to write RTL description of the design in Verilog Hardware Description Language (HDL) and verify the functionality of the design. The design is then synthesized for obtaining the power report. The following sections brief us about the idea of the paper and simulations via testbench.

A. Flow Diagram

Five 7-segment displays are used accepting hexadecimal inputs. At the output, there is an unlock bit which gets high if the "8A20D" is given at the input, else it remains low. A 2-bit counter named "unsuccess" is incorporated to keep a track of unsuccessful attempts. It increments its value upon entering the wrong code. If 3 failed attempts are made, then a burglar alarm's output signal will be activated which otherwise remains at logic low. The idea is well explained in figure 1.

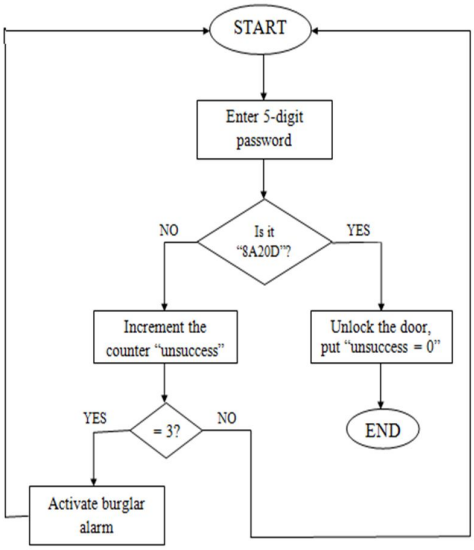

Figure 1. Flow diagram

The main objective behind the proposal is to make hacking of the secret code difficult. To achieve this 7-segment displays have been used which take hexadecimal values. So possible combinations to try from become 16^5, which is equal to 10,48,576 combinations. This reduces the probability of getting correct code within 3 attempts. If any intruder does not succeed in 3 attempts, then there is a burglar alarm that will inform the near-by persons about this theft. Also, the proposed design is simple to implement.

B. Testbench

Testbenches are used for simulating the designs described using some HDL. They are considered a more reliable and preferred choice of the clients for testing a design in contrast to manually applying the test vectors. The outputs generated are user-friendly and in a readable format.

Writing testbenches is worthwhile especially when there are long codes which are to be tested by a huge set of test vectors of many bits. In practical scenarios, the circuits may have, say, 12-bit input. This would mean that one needs to test all of 2^{12}-1 input vectors which is a difficult task for a human. Testbenches can help simulate the designs with ease. They make testing of the designs efficient and less cumbersome, else if any bug is found in physical circuits after manufacturing, then the design cannot be reversed leading to increased designing cost.

The design is simulated by writing the Verilog testbench. The top module is instantiated with properly defined input-output ports. The test vectors for the top module design are specified within the initial block. Here, 7 test vectors are taken to check the functionality of the design. Each input vector will be applied after a delay of 10 nanoseconds.

IV. Results and Discussion

A. Simulation Results

The authentic passcode for unlocking the door is taken as "8A20D". When this code is entered, the unlock bit at the output is set high indicating the door is opened. This is shown in the simulation results of figure 3 during the initial 10ns timeframe. As soon as an invalid code is entered, the door remains in locked state and the counter starts incrementing its value. This is depicted in the figure 2 by applying codes "8A20F" and "7A30E" for the next 20ns. In this time duration, the counter value increments to 1, then 2 and the door remains closed.

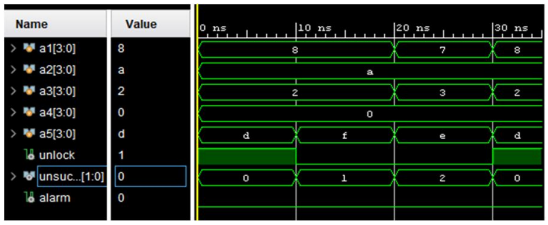

Figure 2. When correct is entered followed by incorrect code

Figure 3 shows the waveforms when correct code '8A20D' is applied and the counter value resets to 0. The door unlocks for the house owner. As the incorrect codes are applied, the counter starts incrementing its value again and the door remains closed. This continues until either the correct code is entered into the system, or the counter reaches its maximum value 3 and pushes the alarm.

Figure 3. When 8A20D is entered after entering wrong code

Figure 4 depicts the case when the incorrect code is entered consecutively for three times. In such a situation, the security lock increments the counter value up to 3. The moment the counter value reaches 3, an "alarm" signal is set at high logic, indicating activation of a burglar alarm. The purpose of the alarm signal is to notify the responsible persons and the neighbors about ongoing break-in into the house.

Once the intrusion is addressed by the system owners, the system can be brought into a reset condition manually. In future, a reset signal can be incorporated in the system that may become activated a few minutes after the burglar alarm starts ringing.

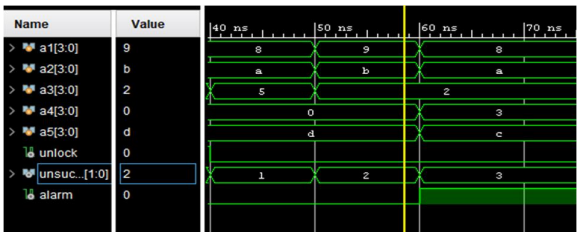

Figure 4. When wrong code is entered 3 times consecutively

Figure 5 shows the summary of on-chip power consumed by the design obtained from the power report after synthesis is done on the Vivado tool. Total on-chip power consumed happens to be 1.726 watt, which is composed of dynamic power (1.642 watt) and static power (0.084 watt).

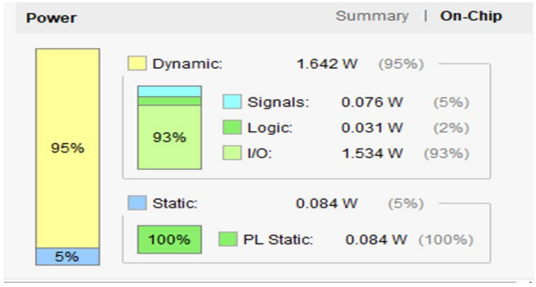

Figure 5. Power consumed

B. Discussion

The proposed idea is similar to the one explained in [6] except for the fact that the design being put forward is meant for implementation on FPGA board having additional functionalities in comparison with an Arduino board. Arduino executes operations in a sequential fashion. With FPGA, we get an advantage of executing multiple operations parallelly at the same time.

The study conducted by Nasir et al. [8] uses slide switches for user-entered passcode which control the LEDs. Accordingly the outputs are displayed on 7-segment and LCD displays. The design comprises two modules which are lock system and decision-making modules. However, this paper uses only 7-segment displays to take the secret code from the owner. Moreover, there is only one module responsible for taking the code, comparing it with the authentic one and making a decision of whether or not to unlock the door.

Another Arduino based security system uses RFID tags [10] with intended applications in Laboratories and Libraries. RFID tags cannot be seen through eyes meaning they can be easily cloned. At times it becomes difficult to read the tags. With the proposed design, no such difficulties will be faced. This password-based system gives the owner a right to change the code anytime for more security so that even if someone has stolen the code, it remains equally difficult for the intruder to get the access.

The idea implemented by K.Saroch et al. [13] uses FSM to implement a password-based system on FPGA and is designed in VHDL. The suggested design uses simpler logic explained in figure 1. The designing is done in Verilog HDL thereby reducing the complexity and length of the code. This makes the design more convenient and user-friendly.

V. Conclusions

The proposed design is successfully simulated in the Xilinx Vivado tool. In this design, we have taken a 5-digital code in hexadecimal format. The secret code can be a 5-digit combination of any number from 0 to F. In future, the length of the actual code can be reduced while keeping it same for others by taking some hexadecimal digits as input and giving a hyphen (-) or underscore (_) symbol at output. Through 7-segment displays, more characters can be included in the secret code other than the hexadecimal digits.

The future scope is vast enough as there are many technologies which can be included in the design for security enhancement. A camera can be incorporated to monitor the persons trying to access the lock. It is not always possible for the home occupants to be present during the ongoing intrusion. Therefore, GSM technology can be added to send alert notifications during break-ins.

The proposed security system is a low-cost and energy-efficient security system that can be easily implemented on any FPGA board using 7-segment displays. It sees applications in doors of smart homes, hospitals and bank lockers. The security system designed will increase the security standards and will promote the concept of independently living a quality life.

ACKNOWLEDGMENT

First of all, I acknowledge the praise to the Almighty God for giving the strength to accomplish this work. I would like to thank my faculty advisor Dr. Shobha Sharma for her essential guidance, support and precious advice. I wish to extend my special thanks to my parents for their inestimable support.

REFERENCES

[1] I. H. Hamzah, M. S. Z. Suhaimi, A. A. Malik and A. F. Rahim, "Design and implementation of HDL remote controller for smart home system", *Indonesian Journal of Eletrical Engineering and Computer Science*, vol. 20, issue 1, pp. 117-124, October 2020.

[2] Li W, Li H, Gong A, Ou Y and Li M., "An intelligent electronic lock for remote-control system based on the Internet of Things", *Journal of Physics: Conference Series*, IOP Publishing, pp. 1-7, 2018.

[3] Yeap KH., "Design of a keyless coded home lock system using Verilog hardware description language", *International Journal of Electronics, Computer and Communications Technologies*, vol. 3, issue 1, pp. 10-16, 2012.

[4] Pavan Mankal, "Verification of 4-Digit Password based Digital Lock using Constrained Randomized Layered Test Bench", *International Journal for Scientific Research & Development*, vol. 6, issue 06, 2018.

[5] M. Tseng, K. Liu, C. Hsieh, S. J. Hsu and C. Chan, "Gesture spotting algorithm for door opening using single wearable sensor," *2018 IEEE International Conference on Applied System Invention (ICASI)*, pp. 854-856, 2018.

[6] Sriharsha B S, Zabiullah, Vishnu S B and Sanju V, "Password Protected Locking System Using Arduino," in *BIJIT – 2016, January - June, 2016*, vol. 8, issue 1.

[7] S. B. Saleh, S. B. Mazlan, N. I. Hamzah, A. Z. Karim, M. S. Zainal, S. A. Hamzah, D. B. Nor and H. B. Poad, "Smart home security access system using field programmable gate arrays", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 11, issue 1, pp. 152-160, July 2018.

[8] N. M. Nasir, I. H. Hamzah, A. A. Malik, M. H. Abdullah, A. F. Rahim and A. A. A. Samat, "Electronic combination lock system using Verilog HDL", *International Journal of Advanced Technology and Engineering Exploration*, vol. 8 (75), February 2021.

[9] Y. Yu, "A practical digital door lock for smart home," *2018 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-2, 2018.

[10] H. Prasad, R. K. Sharma and U. Saini, "Digital (Electronic) Locker", *2020 First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA)*, pp. 1-4, 2020.

[11] H. Alnabhi, Y. A. Naamani, M. A. Madhehagi and M. Alhamzi, "Enhanced security methods of door locking based fingerprint", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, issue 3, pp. 1173-1178, January 2020.

[12] S. Nath, P. Banerjee, R. N. Biswas, S. K. Mitra and M. K. Naskar, "Arduino based door unlocking system with real time control", *2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 358-362, 2016.

[13] K. Saroch and A. Sharma, "FPGA based system login security lock design using finite state machine", *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, vol. 5, issue 3, pp. 70-75, 2013.

[14] S.Subba, B.Dahal, N.Rai, R.Banstola, S.Das and S.P.Tamang, "FPGA based Security Login System using GSM with OTP Generation", *International Journal of Advanced Engineering Research and Science (IJAERS)*, vol. 4, issue 2, 86-90, 2017.