https://dx.doi.org/10.22161/ijaers.4.2.18 ISSN: 2349-6495(P) | 2456-1908(O)

FPGA based Security Login System using GSM with OTP Generation

Samiksha Subba[1], Bhawana Dahal[1], Nirmal Rai[2], Rochan Banstola[2], Suman Das[2], Surya Prakash Tamang[2]

[1]B.Tech Student, ECE Dept., Sikkim Manipal Institute of Technology, Sikkim-737132, India
[2]Assistant Professor, ECE Dept., Sikkim Manipal Institute of Technology, Sikkim-737132, India

Abstract— *Security of system is major concern in this age of high-tech infrastructure. In today's materialistic world, security holds an in dispensable place. Security in every aspect is highly desirable may be at home or at office etc. as thefts and robberies are increasing day by day. To overcome this security threat, a security system has been proposed using GSM technology, by generating One Time Password and implementing in FPGA. As FPGAs offer all of the features needed to implement most complex designs. This security system activates, authenticates and validates the user and then unlocks the system. This project attempts to create security login systemwhere the user is granted access if he enters the correct predefined password and is denied access if he enter the wrong password. When password is entered GSM gets activated and send SMS to user's mobile phone, after authentication random OTP is generated and should be verified such that the system gets accessed. In every 3 minutes this OTP verification code will change and is valid for 3 minutes. The outcome of each and all would be available in the LCD of the Spartan 3E board. VHDL codes are used to design this system using Xilinx ISE 9.2i.*

Keywords— FPGA, PS/2 KEYBOARD, GSM, OTP, VHDL.

I. INTRODUCTION

In this project we implement a system security on FPGA using GSM and generating OTP because at present time security system has become one of the most important technologies in this global world. Nowadays there is demand for more efficient security systems to avoid access of unauthorized persons. In recent system a unique password is set to open locker, which is only known to authorize person. The user uses this password again and again so somebody can hack that password and also if password leaks then it affect security of system. Development of an alert system; triggered on an offence to unlock the digital lock system in the door assembly. The prototype developed in this research work sends a Short Message Service (SMS) to the house or office owner's cellular mobile phone; as soon as any unauthorized person tries to unlock the digital lock[1].Most of the secure systems are designed using SRAM based FPGAs with additional security features provided by the manufactures[2]**.** Implementation a low-power system where the customer will be granted access to his locked car as he approaches the vehicle. With such a system, the advantages of keyless access will be accomplished with only passive involvement from the client [3].FPGA based system login security lock design using finite state machine introduces the security technology for machines or objects. An automatic Security System Login Lock using FSM based on FPGA has been developed which can be done with the help of XILINX software. VHDL is used in this research paper to design SYSTEM LOGIN SECURITY LOCK. Here, the lock can only opened when the desired code (password) is entered or the given sequence is detected by the system. The logic of the system is developed in the form of state diagram with the help of Xilinx state CAD tool [4]. FPGA based systems are prone to different types of attacks, like cloning of bit streams, modification of bit stream, unauthorized usage of FPGA based system etc. Several techniques are proposed to overcome the problem of bit-stream copying. FPGA bit streams are encrypted to avoid copying of FPGA bit streams. On chip decryption must be provided so that, the encrypted bit streams are converted back to its original form. With the help of an encryption key, bit streams are encrypted and sent to the FPGA and encrypted bit streams are converted back to its original form with the help of a decryption key. In the case of control word based FPGA systems, bit streams are not encrypted and an intruder who copies the bit stream may download this copied bit streams into his FPGA to perform some function [5].

https://dx.doi.org/10.22161/ijaers.4.2.18 *ISSN: 2349-6495(P) | 2456-1908(O)*

In today's materialistic world, security holds an in dispensable place. There is a need of security in almost every sector of society viz. offices, houses, banks, cyber etc. as thefts and robberies are increasing day by day. Increase in usage of network based system has made the current security system old dated as the hackers and attackers of network system is on rise with new and modern attack methodologies . This has necessitated the need of more secure ways of communication.To overcome this security threat, a security system has been proposed using FPGA, GSM technology and by generating One Time Password (OTP).

II. PROBLEM DEFINITION AND PROPOSED SOLUTION

In our project there are different interfacing circuits, PS2 keyboard with FPGA and GSM with FPGA. While Interfacing FPGA with PS2 keyboard and with GSM, the baud rate should be matched (9600 bps).The complexity of coding substantially increases, but once programmed the module works at its robust best since it is a dedicated embedded system and not a general purpose computer. The design procedure involves identifying and assembling all the required hardware and ensuring safe interfacing between all the components. Then we have the coding process which has to take care of the delays between two successive transmissions.

III. BASIC ARCHITECTURE

FPGA find applications in many domains of automation. The domain of security is what this project tries to implement by incorporating FPGA. Protection of personal belongings becomes a daunting task. Thus, a simple system that can provide protection along with added flexibility in design would be an added advantage. There are various types of security providing techniques using hardware and software medium. However, they happen to be little rigid and application specific. Security in research centers as well as big offices remains a main attraction. Thus, if a system incorporating flexibility is designed it will create a spark pushing digital technology of soft processing even further.

In this project we implement simple security login using GSM system that identifies the entered code and allows an individual, an access inside a premise whereby not allowing an access if code is unidentified. To achieve this task of unlocking system, VHDL code is written in Xilinx ISE and programmed into the FPGA of the Spartan 3E starter kit of the Spartan boards family. A password is entered, if this password matches with the predefined password, GSM sends one time password (OTP) to registered mobile number. The person unlocking the system needs to enter the OTP. If the OTP to user's mobile phone matches with the entered OTP only then the system gets unlocked.

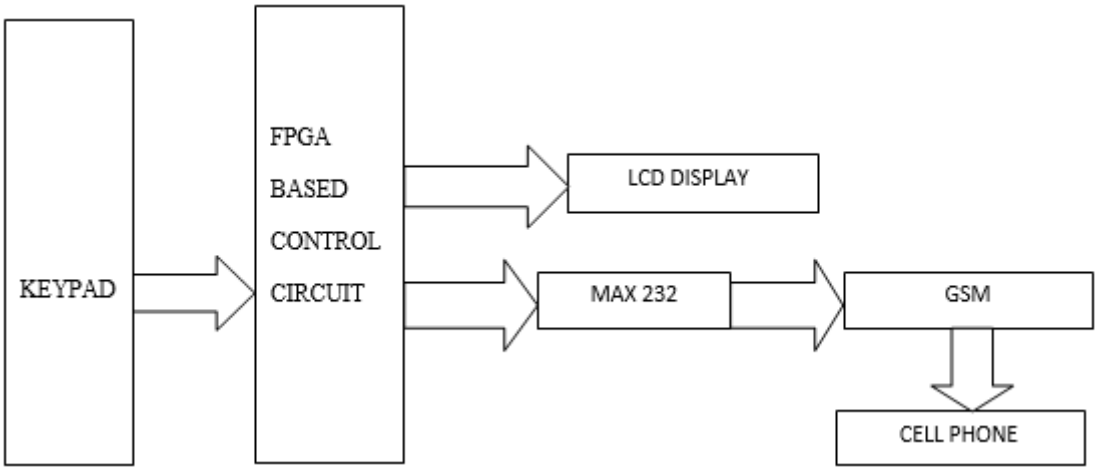

Fig. 1: Basic architecture of FPGA based Security login system using GSM

IV. IMPLEMENTATION

In implementing 'FPGA based security system based on GSM with OTP generation', resources used include Spartan 3E kit and GSM. The design is not too complex, however long VHDL code is used to implement the system. Selection of language 'VHDL' lied mostly on its easiness and our novice knowledge to other Hardware descriptive languages.In this project the code is written in Xilinx software and when code is run on Spartan 3E kit, LCD displays 'Enter Password'. The predefined password is already stored in the system. User need to enter the correct predefined password, if the entered password matches with the predefined password then LCD displays 'Access Granted' and GSM sends OTP(one time password) to user's

https://dx.doi.org/10.22161/ijaers.4.2.18 *ISSN: 2349-6495(P) | 2456-1908(O)*

phone number. If the predefined password does not match with the entered password then LCD displays 'Access Denied'. If the person unlocking the system enters the correct OTP, only then the system gets unlocked and LCD displays 'Access Granted'. If not again OTP is generated and send to user's mobile number.In this project apart from Spartan 3E FPGA kit we have also interfaced the board with keyboard and GSM. The keyboard is used to enter the password to the Spartan 3E kit. If the predefined password entered is correct then the Spartan 3E kit sends OTP to GSM. Further, GSM sends OTP to registered phone number.

V. DESIGN

There are various components used along with the FPGA such as keyboard and GSM. GSM is interfaced to Spartan 3e kit using AT commands using VHDL and keyboard is also interfaced using hardware descriptive language VHDL. VHDL codes were developed to integrate all the different components together and provide a working of the overall system. The concept of design and individual modules of the design are further explained in detail here.The hardware implementation is depicted in Fig.2:

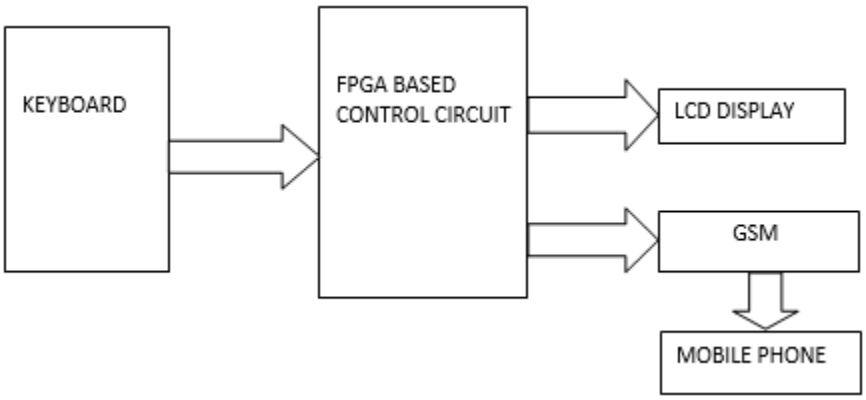

Fig.2: Block Diagram of interfacing components

The figure depicts the flow of signals in the program. The FPGA based control circuit operates the program connecting all other components. The keyboard is used to enter the password. As the FPGA takes in the password it checks it with the password stored in the program. Thus the FPGA decides whether the password is correct or false. Then FPGA sends OTP to GSM if the entered password is correct.GSM further sends the OTP to user's mobile number. The person unlocking the system needs to enter the correct OTP through keyboard in order to access the system.

This system is more secured as compared to other security system because here we are generating one time password. Only the person whose phone number is registered has access to the one time password.

VI. RANDOM ONE TIME PASSWORD GENERATION

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication.

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to reply attacks. This means that a potential intruder who manages to record an OTP that was already used to login to a service will not be able to abuse it, since it will no longer be valid.

OTP generation algorithms typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for hash. This is necessary because otherwise it would be easy, to predict future OTPs by observing previous ones.

There are two principal methods used to generate random numbers. One measures some physical phenomenon that is expected to be random and then compensates for possible biases in the measurement process known as True Random Number Generators (TRNGs). The other uses mathematical algorithms that produce long sequences of apparently random numbers, which are in fact completely determined by an initial value (seed) known as Pesudo Random Number Generators (PRNGs).

https://dx.doi.org/10.22161/ijaers.4.2.18 *ISSN: 2349-6495(P) | 2456-1908(O)*

In our project we have used Pesudo Random Number Generators (PRNGs) to generate One Time Password. A pseudorandom number generator (PRNG),is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random. Although sequences that are closer to truly random can be generated using hardware random number generators, pseudorandom numbers are important in practice for simulations.

A PRNG can be started from an arbitrary starting state using a seed s. It will always produce the same sequence thereafter when initialized with that state. The maximum length of the sequence before it begins to repeat is determined by the size of the state. However, since the length of the maximum period doubles with each bit of 'state' added, it is easy to build PRNGs with periods long enough for many practical applications.Most pseudorandom generator algorithms produce sequences which are uniformly distributed by any of several tests.

The following algorithms of pseudorandom number generators are:-

- Blum BlumShub
- Inversivecongruential generator
- ISAAC (cipher)
- Lagged Fibonacci generator
- Linear congruential generator
- Linear feedback shift register
- Mersenne twister
- Multiply-with-carry
- Well Equidistributed Long-period Linear
- Xorshift

For generating One Time Password, we have used linear feedback shift register (LFSR) algorithm.

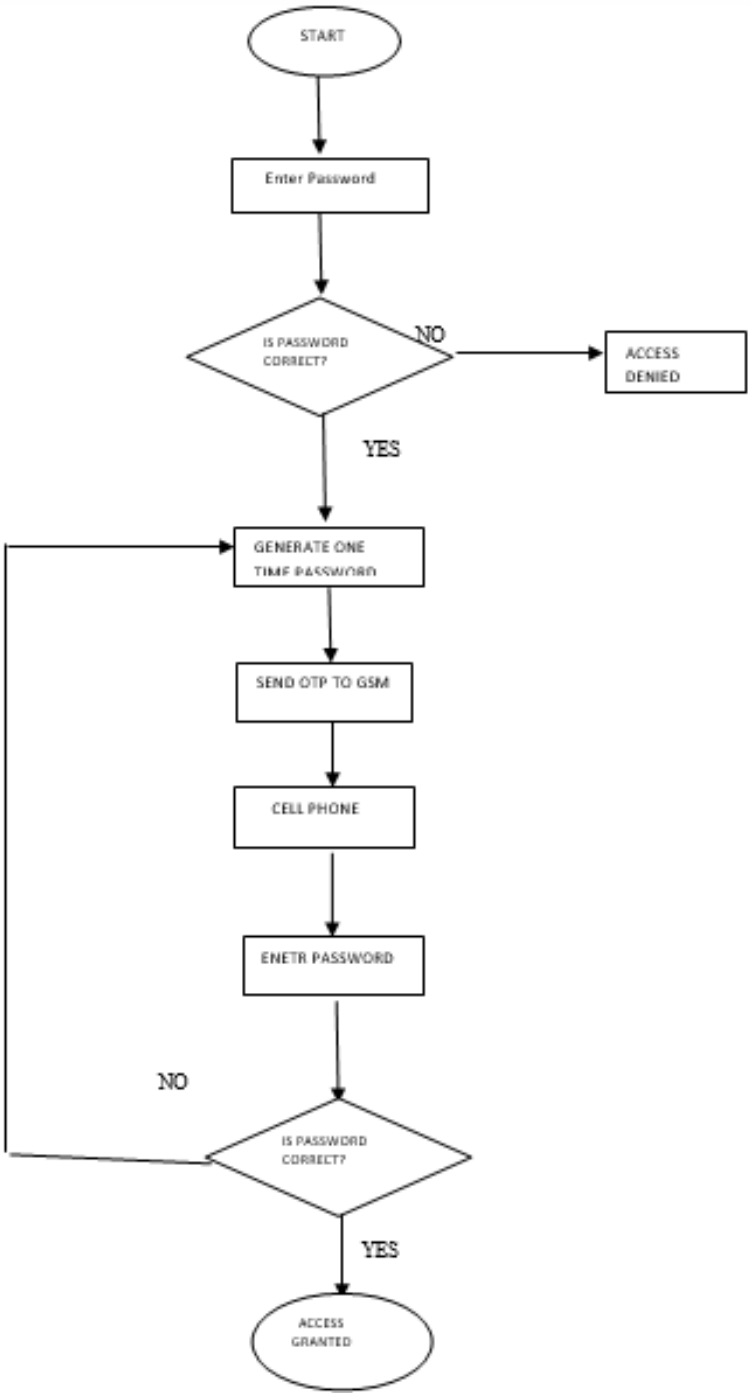

Fig. 3: Overall flow chart of the entire project.

VII. CONCLUSION

The development of the project was a learning experience for all who were involved. The project taught the basics of the communications and the effectiveness of using a FPGA board. The programming and interfacing program with FPGA was a challenge and it took some time for obtaining

https://dx.doi.org/10.22161/ijaers.4.2.18 *ISSN: 2349-6495(P) | 2456-1908(O)*

the desired output. But while building the circuit utmost care should be kept of the circuit connections as any loose connections will lead to loss of data or no transmission at all.

The FPGA board was used because the proposed FPGA based implementation offers hardware flexibility and speed.

VIII. FUTURE SCOPE

We can enhance the security level of One Time Password by encrypting it and logging the user by forwarding the encrypted OTP with Password to the system. It increases the security level of the system. In future, face recognition and GSM based security system can be made to block the larceners from offensive attack on locker system.

REFERENCES

[1] P.K. Gaikwad, "Development of FPGA and GSM based Advanced Digital Locker System", International Journal of Computer Science and Mobile Applications, Vol.1 Issue. 3, September- 2013

[2] Gurjit Singh Walia, GajrajKuldeep, Rajiv Kapoor, A K Sharma, NavneetGaba **"**FPGA Based Secure System Design-an Overview" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, January 2012.

[3] Dr. S .N. Singh, Jayendra Kumar, Ravi Pratap Singh and Sanjay Kumar Department of Electronics and Communication Engineering, National Institute of Technology, Jamshedpur, India "FPGA Based Autonomous Vehicle Locking System- A Smart Door Lock" International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.

[4] Kavita Saroch, Abhilasha Sharma, "FPGA Based System Login Security Lock Design Using Finite State Machine", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p- ISSN: 2278-8735. Volume 5, Issue 3 (Mar. - Apr. 2013), PP 70-75, www.iosrjournals.org

[5] Mr. Binu K Mathew, Dr. K.P Zachariah,"New techniques to enhance FPGA based system security", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 1, Issue 1, July 2012.