IMPLEMENTATION OF FIPS 140-2 STANDARD TAMPER (EVIDENCE/DETECTION) FOR FPGA BASED SYSTEMS

By

Sara Zia

Muneeba Sirshar

Zubair Rasheed

Submitted to the Faculty of Electrical Engineering, Military College of Signals National University of Sciences and Technology, Rawalpindi in partial fulfilment for the requirements of a B.E Degree in Telecom Engineering
JUNE 2015

CERTIFICATE

It is certified that the work contained in this thesis entitled **"Implementing FIPS 140-2 (Tamper Evidence) standard for FPGA based systems"** carried out by Sara Zia, Muneeba Sirshar and Zubair Rasheed under the supervision of Asst. Prof. Mian Muhammad Waseem Iqbal for the partial fulfillment of degree of Bachelors of Telecom (Electrical) Engineering is correct and approved.

X

Asst. Prof. Muhammad Waseem Iqbal
Project Supervisor

Dated:

ABSTRACT

Due to technological advancements, tampering has become one of the most addressed issue in industrial world. The objective of tamper evident design is to make a device resistant to all possible tamper events. This report describes possible techniques to make a system tamper evident. It is integrated with firewall implemented on Field Programmable Gate Array chip (FPGA) and deals with the physical tampering of the system. Design scheme consists of modules both external and internal to FPGA. It also describes authorization mechanism for the system. This project meet level 2 and level 3 of Federal Information Processing Standard (FIPS) 140-2 issued by National Institute of Standards and Technology (NIST). In future we will work on level 4 of FIPS 140-2 Standard. It involves fault induction, power analysis and side channel attacks.

DECLARATION

No portion of the work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere.

DEDICATION

In the name of Allah, the Most Merciful, the Most Beneficent

To our parents, without whose unflinching support and unstinting cooperation,a work of this magnitude would not have been possible

ACKNOWLEDGEMENTS

To begin with, there is no greater guide than **ALLAH (SWT)** Himself and we feel blessed that He gave us enough strength to complete this project well in time.In addition to this, we all would deeply and genuinely like to thank out supervisor Asst. prof Waseem Iqbal for his persistent guidance and continuous support.We would also like to extend our profound recognition to Dr.Mehreen Afzalwho is our co supervisor and always helped us, whenever we needed her.

Table of Contents

Chapter1: Introduction 1
1.1 Problem Statement.....1
1.2 Objective.....1
1.3 Salient Features of the Project.....2
1.4 Scope and Deliverables of the Project.....3
Chapter 2: Literature Review.....3
2.1 Authentication Protocols.....3
2.1.1 Biometric Based Authorization.....3
2.1.2 Optical Based Authorization.....5
2.2 Security Protocols.....6
2.2.1 Motion Sensors.....6
2.2.2 Screw Protection …….……....6
2.2.3 Password Protection …….……....7
2.2.4 Deice Id Identification …….……....7
Chapter 3: Software Requirement Specification.....7
3.1 Biometric Based Autorization.....7
3.2 Optical Based Authorization.....9
3.3 Motion Sensor.....10
Chapter 4: Design and Development…….....11
4.1 Basic Design Scheme.....11
4.1.1 Biometric Based Authorization.....11
4.1.2 Optical Based Authorization.....13
4.1.3 Motion Sensor 18
4.1.4 Password Protection.....19
4.1.5 Screw Protection 20
4.2 Hardware Requirements ……....20
4.2.1 Biometric Based Authorization ……..…20
4.2.2 Optical Based Authorization.....21

4.2.3 Screw Protection…….....21

4.2.4 Motion Sensor…….....21

4.2.5 Password Protection…….21

Chapter 5: Project Analysis and Evaluation.....21

5.1 Biometric Based Authorization……..22

5.2 Optical Based Authorization……..24

5.3 Motion Sensor……25

5.4 Interfacing……..25

Chapter 6: Future work 26

Chapter 7: Conclusion 27

7.1 Overview ……...27

7.2 Objectives Achieved …….27

7.3 Contribution …….....27

7.4 Limitations ……....28

7.5 Applications ……..……....28

BIBLIOGRAPHY 29

Appendix A-Project Proposal ……..……....30

Appendix B-TIME LINE FOR THE PROJECT ...32

Appendix C-Cost Break Down …….33

LIST OF TABLES

Table 3-1Coding Specs of Biometric Based Authorization Module…….9

Table 3-2 Coding Specs of Optical Based Authorization.....10

Table 3-3 Software Specs of Motion Sensor.....10

Table 3-4 Coding Specs of Motion Sensor ….....10

Table 3-5 Coding Specs of Controller.....11

Table 4-1 Comparison of PUF with The Standard PUF…..……...16

Table 5-1Comparison of Various BiometricBased Modules Technologies……..22

Table 5-2 Comparison of Technologies Considered For Biometric Based Authorization …….……23

Table 5-3 Comparison of Technologies Considered for Biometric Based Authorization Module.....24

Table 5-4 Comparison of Technologies Considered for Motion Sensor Module……..25

LIST OF FIGURES

Figure 1-1 Overall Design Scheme.....2

Figure 1-2 General Operation of FPGA Security Mechanism.....3

Figure 2-1 Basic Work Flow of Biometrics.....4

Figure 2-2General Operation of Finger Print Authorization.....4

Figure 2-3 General overview of PUF.....5

Figure 4-1 Work Flow of Biometric Based Authorization.....12

Figure 4-2 Diagrammatic Work Flow of PUF.....14

Figure 4-3 Work Flow of Biometric.....14

Figure 4-4 Ov7670.....15

Figure 4-5 Arduino Uno.....17

Figure 4-6 Work Flow of motion sensors.....18

Figure 4-7 Basic Block Diagram of Motion Sensor.....19

Figure 4-8 Basic Block Diagram of Motion Sensor.....20

Figure 5-1 Enrolment of Finger Print.....23

Figure 5-2 Verification of Finger Print.....24

Figure 5-3 Testing of Motion Sensor.....25

CHAPTER 1: INTRODUCTION

1.1 Problem Statement:

Designing a security mechanism for FPGA based system to detect any kind of physical tampering. This security system will be able to integrate with any device based on FPGA. It will provide security to the cryptographic keys and plain text data stored in the FPGA. This system will be meeting the security requirements of FIPS 140-2 standard level 2 and level 3 [1].

1.2 Objective:

The objective of this project is to make such a system that provides security to the FPGA based system. This project aims to provide physical security to a firewall based on FPGA in accordance with standards of FIPS 140-2 [1].The target of the project is to save the box from any unauthorized user. This system can be used in military equipment as well as the industrial equipment with high security requirements. It is based on hardware devices for security of box which will be integrated with FPGA where FPGA will be programmed using Verilog hardware defined language. The system will also include highly reliable authorization system to give access to the authorized user to the device.

Some of the highlighted objectives of this project are.

- Development of reliable hardware security system
- To save the device form intruders.
- To provide access to authorized users only.
- To achieve the security requirements of FIPS 140-2 standard [1].
- Cost Effectiveness.

1.3 Salient Features Of The Project:

Based on the requirements of security for the CRP's (Cryptographic parameters) in FPGA, the security system will be developed using different sensors integrated with some mechanism to alert the authorized user about the temper event. Also the mechanisms for the authorization are developed namely PUF (physically un clonable function) along with the finger print sensor to make authorization system more strong and reliable [2]. All above systems will be interfaced with FPGA directly and some through microcontrollers

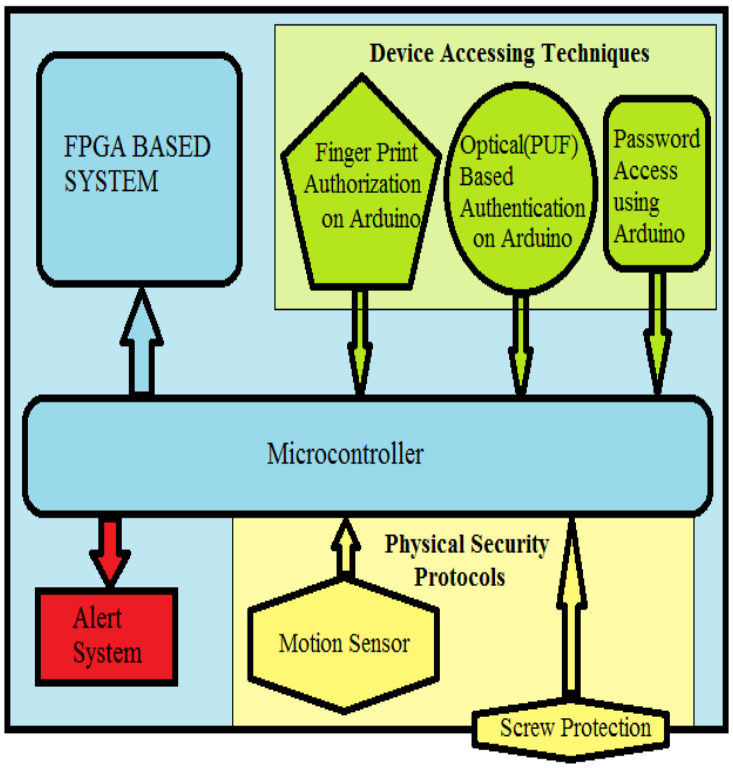


Figure 1-1 Overall Design Scheme

As shown in the above figure, the FPGA will be secured using the number of sensors integrated with FPGA. Alert will be generated if any one of them gives response. Access shall be provided only to authorize user overriding all these detection mechanisms. The authorized user will be identified role as well as identity based and different users will be given access to the device to a limited functionality.

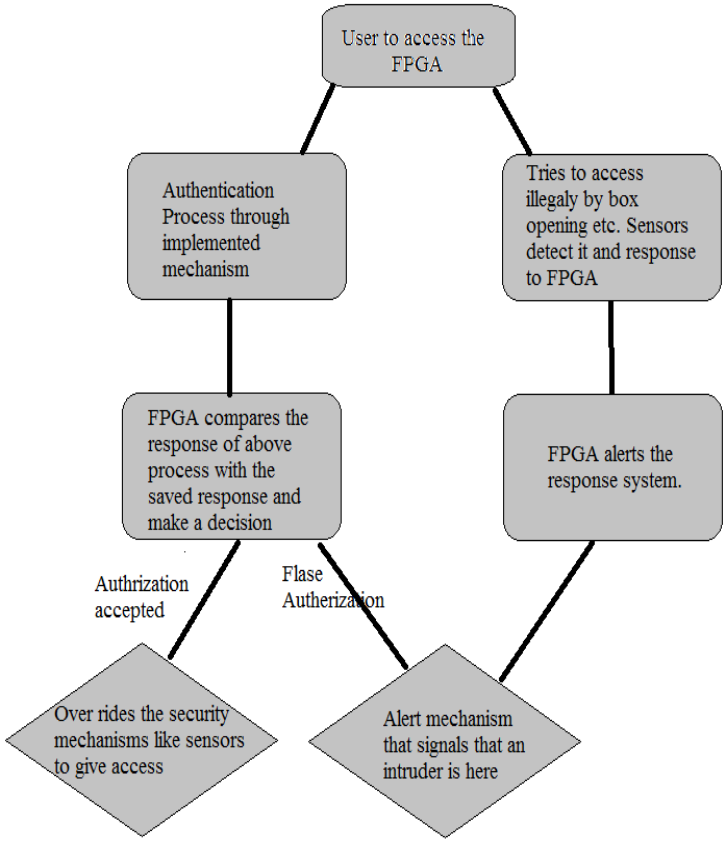


Figure 1-2 General Operation of FPGA Security Mechanism

1.4 Scope And Deliverables Of The Project:

This project aims to develop a higher level of security for FPGA. After implementation of this on any device the device will be amongst the few devices that meet the FIPS 140-2 standard by NIST [1].

CHAPTER 2: LITERATURE OVERVIEW

2.1 Authentication Protocols:

2.1.1 Biometric Based Authorization:

A fingerprint an impression of the friction ridges of all or any part of the finger. Fingerprint recognition systems use characteristics from these ridges (they are also called fingerprint features) to differentiate one fingerprint from another [3].

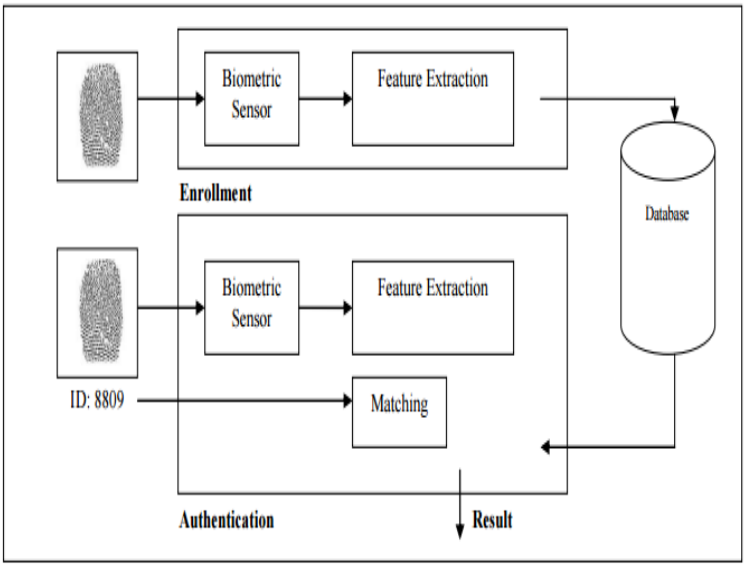


Figure 2-1 Basic Work Flow of aBiometric

Basic Design:

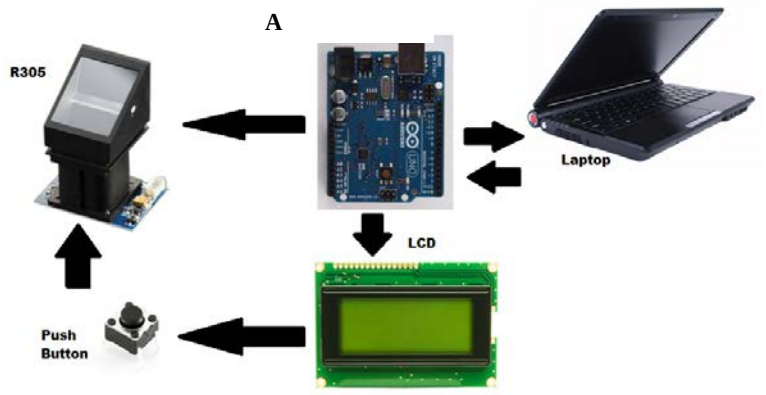


Figure 2-2 General Operation of Finger Print Authorization

Finger print authorization is implemented using an Arduino uno board and an optical sensor. R305 is an optical based finger print sensor that can store and compare up to 162 finger prints. It is used to capture an image of the finger and sends it to Arduino board through UART 232 interfacing.

This is done by creating a virtual serial port using Software serial. A personal computer is connected to Arduino on the other end through USB interface. For the purpose of enrolment a unique identification pin number is provided by the user through the personal computer that is connected to Arduino board. 16 by 4 LCD is used to display the unique identification pin number during the verification process.

2.1.2 Optical Based Authorization:

It is a strong and reliable method of authentication and it uses a simple mechanism of laser and sensors along with refractive particles in a glass plate used as a token for the authentication [2]. The image appeared through scattering Token on sensors are transformed to bit string.

As shown in figure. There are two possibilities of its making one is using sensor grid while other is using CCD camera. We will be possibly using the sensor grid.

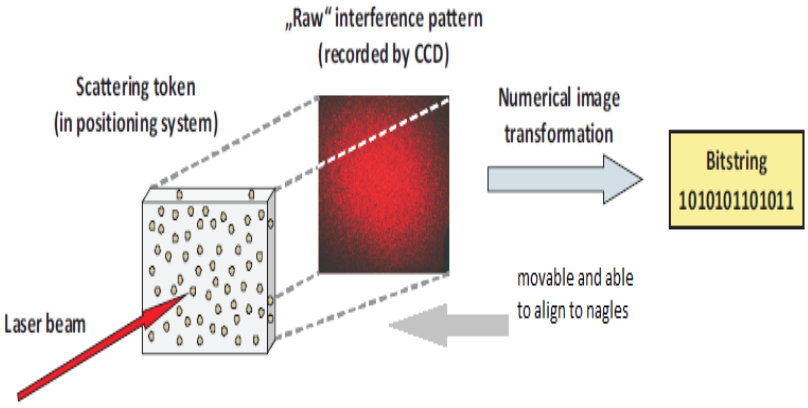


Figure 2-3General overview of PUF [2].

2.2 Security Protocols:

2.2.1 Motion Sensors:

Motion sensors are the devices that are used to detect and measure any motion caused in the device. They mainly consist of Accelerometer and Gyroscope. Accelerometer measures any non-gravitational motion of the device. It basically consists of microscopic crystals with give output in voltage once they sense vibration due to motion while Gyroscope gives output once it senses any rotational motion with respect to Earth's gravitational motion

Constraint Faced During Implementation

- The motion sensor proposed earlier in the project proposal was ADXL 345 but due to shortage of availability, ADXL 335 was used as its replacement. This sensor had more sensitivity which added more security to the system.
- Proteus software does not contain any library for any motion sensor hence two different simulating software had to be used to test the design.
- Both modules of MPU 6050 were planned to be implemented earlier but exact values of the tilt could not be achieved easily due to noise and other factors so accelerometer module is implemented only and comparison between different output values achieved is used to activate the alarm.

2.2.2 Screw Protection:

The casing of the devices is protected by this module of the design. The system is activated at low level signal using IC 1404. The output of the system is interfaced to microcontroller ATMEGA 32. The input of the system is connected to the push buttons which are adjusted in such a way to give to give high level signal as long as screws are in contact with them.

2.2.3 Password Protection:

The password protection is being provided using Arduino board for the time being in which four users are allowed to access the device on the basis of correct password. We also tried to implement the password protection directly connecting the keyboard on FPGA but due to sensitivity issues we could not do it. The codes for FPGA are also given in appendix-B.

2.2.4Device ID Identification:

For this module we used command prompt based to provide basic commands using the B scan mode. Through this procedure, we obtain a unique device ID. This device ID is stored in DDR3 RAM of vertex 6 FPGA. On the chip start up, this unique ID is read and is compared with already stored value. If the comparison returns a true value, a blinking LED. The codes for this module have been attached in Appendix B.

CHAPTER 3: SOFTWARE REQUIREMENTS

3.1 Biometric Based Authorization:

The codes implemented in Arduino UNO have been attached in Appendix B for reference.

P	**C**	**S**	**L**
u	**o**	**p**	**i**
r	**m**	**e**	**b**
p	**m**	**c**	**r**
o	**a**	**i**	**a**
s	**n**	**f**	**r**
e	**d**	**i**	**y**
		c	
	u	**a**	**U**

	s **e** **d**	**t** **i** **o** **n**	**s** **e** **d**
C r e a t i n g s o f t w a r e s e r i a l	S o f t w a r e S e r i a l m y S e r i a l (2 ,	V i r t u a l s e r i a l p i n s a r e c r e a	< S o f t w a r e S e r i a l . h >

	3) ;	t e d a t p i n 2 a n d 3	
I n i t i a l i z i n g	L i q u i d C r y s t a l	I n i t i a l i z i n g	< L i q u i d C r y s t a

p i n s	l c d (9 , 8 , 7 , 6 , 5 , 4) ;	t h e l c d p i n s	l . h >
S e t t i n g	l c d . s e t C	S e t s t h e	< L i q u i d C

LCD curser	ursor(0,0)	curser on LCD	rystal.h>
Interfacing the	constintbuttonPi	Push button is m	<Softtwareserial.

p u s h b u t t o n	n = 1 0 ;	a d e t o w o r k o n t w o l e v e l s	h >
S e r i	S e r i a	I n i t i	< S o f t

all communication with personal	l.begin(9600);	alizes serial communication with	wareSerial.h>

computer		personalcomputer	
Displayon LC	Serial.printl	Connecting LC	<Liquid Crysta

D	n (" f i n g e r t e s t ") ;	D t h r o u g h s e r i a l i n t e r f a c e	l . h >
S e r i a	f i n g e	d a t a	< A d a f

l c o m m u n i c a t i o n t h r o u g h s e n s o r	r . b e g i n (5 7 6 0 0)	r a t e f o r t h e s e n s o r s e r i a l p o r t	r u i t _ F i n g e r p r i n t . h >

Setting digital pins of control	digitalWrite(ledPin, HIGH);	Digital pin is set high	<Softwareserial.h>

l e r			
V e r i f i c a t i o n	f i n g e r . v e r i f y P a s s w o r d ( )	M a t c h i n g t h r o u g h d a t a b a s e	< A d a f r u i t _ F i n g e r p r i n t . h >
D	d	P	<

e l a y	e l a y (5 0) ;	r o v i d e d e l a y t o k e e p d i s p l a y o	S o f t w a r e S e r i a l . h >

		n	
E n r o l m e n t	g e t F i n g e r p r i n t E n r o l l (u i n t 8 _ t	G e t t i n g a n e w u s e r e n r o l l e d	< A d a f r u i t _ F i n g e r p r i n t . h >

	id)		
Convert sion to grey scale	finger.image2Tz(1)	The dots in the grid are co	<Adafruit_Fingerprint.h>

		nverted to grey scale	
Searching	finger.fi	Searching	<Adafruit

	n g e r F a s t S e a r c h ( )	 t h r o u g h t h e d a t a b a s e	_ F i n g e r p r i n t . h >

Table 3-1Coding Specs of biometric based authorization module

3.2 Optical Based Authorization

The coding is done using the Arduino board which is given in Appendix B. The libraries used for this camera interfaceare given in the table.

	Speci	**Library**

	ficati on	**Used**
C r e a t i n g s o f t w a r e s e r i a l	Virtu al serial pins are creat ed at pin 2 and 3	<Software Serial.h>
I n i t	Defin es the varia	<ov7670. h>

i a l i z a t i o n t h e c a m e r a t o c a p t u r	bles to be used in com muni catio n	

e .		
R e g i s t e r i n i t i a l i z a t i o n	Initia lizes the regist ers in ov76 70	<ov7670_ reg.h>

Table 3-2 Coding Specs of optical based authorization module

3.3 Motion Sensor:

Complete codes are provided in appendix B. Following table gives specifications of software used to implement this module

Software used	**Version**
Atmel Studio	6.0
Proteus (ISIS)	7.7

Table 3-3 software Specs of motion sensor module

Following table specifies libraries used.

Library	**Used**
avr/io.h	To enable input and output for AVR microcontroller
util/delay.h	To include delay in commands

Table 3-4 Coding Specs of motion sensor module

Following Table specifies important functions coded into ATMEGA32.

TWIM_init (bitrate)	To initialize I2c mode of ATMEGA 32
TWIM_Wri	To activate

teRegister(107,0)	microcontroller from sleep mode
MPU6050_ ReadGyro(axis)	To read output values from gyroscope
MPPU6050 _ReadAccel (axis)	To read output from accelerometer

Table 3-5 Coding Specs of controller

CHAPTER 4: DESIGN AND DEVELOPMENT

4.1 Basic Design Scheme:

4.1.1 Biometric Based Authorization:

A fingerprint an impression of the friction ridges of all or any part of the finger. Fingerprint recognition systems use characteristics from these ridges (they are also called fingerprint features) to differentiate one fingerprint from another [3].Finger print authorization is implemented using an Arduino uno board and an optical sensor. R305 is an optical based finger print sensor that can store and compare up to 162 finger prints. It is used to capture an image of the finger and sends it to Arduino board through UART 232 interfacing. This is done by creating a virtual serial port using Software serial. A personal computer is connected to Arduino on the other end through USB interface. For the purpose of enrolment a unique identification pin number is provided by the user through the personal computer that is connected to Arduino board. 16 by 4 LCD is used to display the unique identification pin number during the verification process.

Flow Diagram:

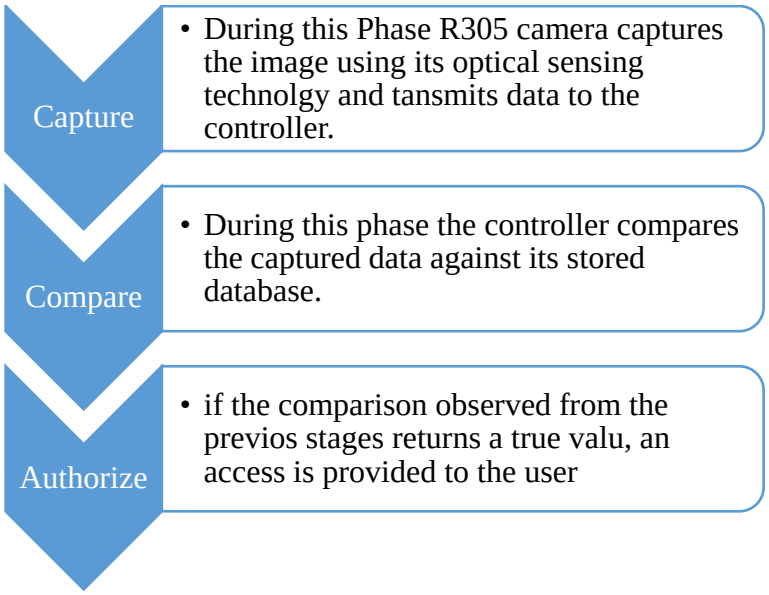


Figure 4-1 Work Flow of Biometric Based Authorization

There are various phases for this process

1. Enrollment:

Fingerprint enrollment is a process during which features from a finger are extracted and saved as a fingerprint template for a future comparison against other fingerprint templates. The following instructions describe a typical fingerprint enrollment scheme:

1. Get a person's identification number.
2. Capture a person's fingerprint using a fingerprint scanner.
3. Extract a fingerprint features from a fingerprint image.
4. Associate a person with his fingerprint.
5. Save extracted features (a template) to a database.

2. Verification:

Fingerprint verification is a process during which a scanned fingerprint is compared with the one saved to a database and is decided whether the two match. The following scheme is usually used for a fingerprint verification:

- Get a person's identification number.
- Capture a person's fingerprint using a fingerprint scanner.
- Extract a fingerprint features from a fingerprint image for the purpose of verification.
- Get a fingerprint template (the one that was saved to a database earlier) by identification number
- Compare two fingerprints: the one that was scanned with the one thatwas saved to database.
- Perform an action according to the verification result (e.g. unlock a computer if two fingerprints matches).

4.1.2 Optical Based Authorization:

It is a strong and reliable method of authentication and it uses a simple mechanism of laser and sensors along with refractive particles in a glass plate used as a token for the authentication [2]. The image appeared through scattering Token on sensors are transformed to bit string.

As shown in figure. There are two possibilities of its making one is using sensor grid while other is using CCD camera. We will be possibly using the sensor grid.

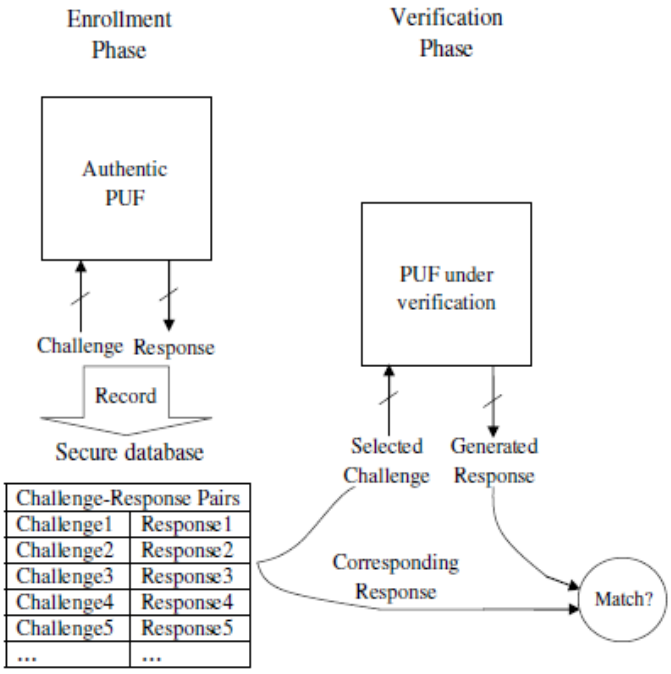


Figure 4-2Diagramatic Work Flow of PUF [2].

Flow Diagram:

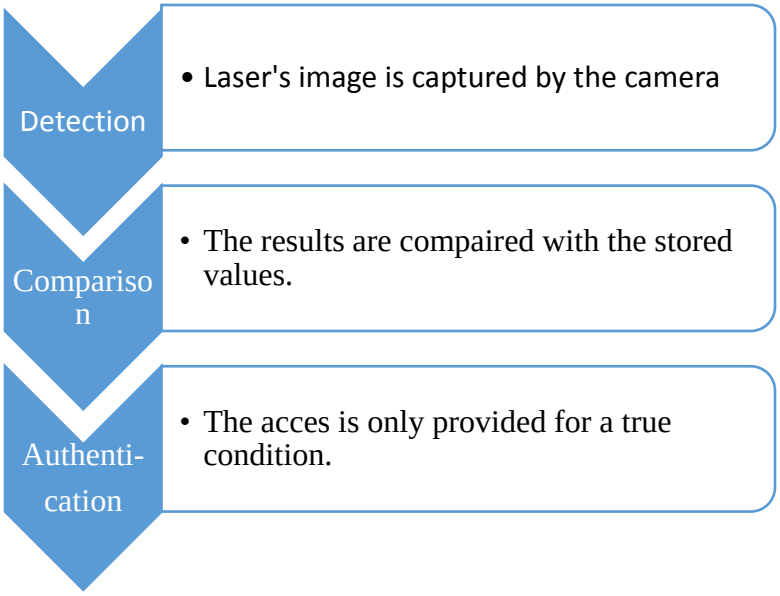


Figure 4-3 Work Flow of PUF

Equipment Used:

(i) camera ov7670:

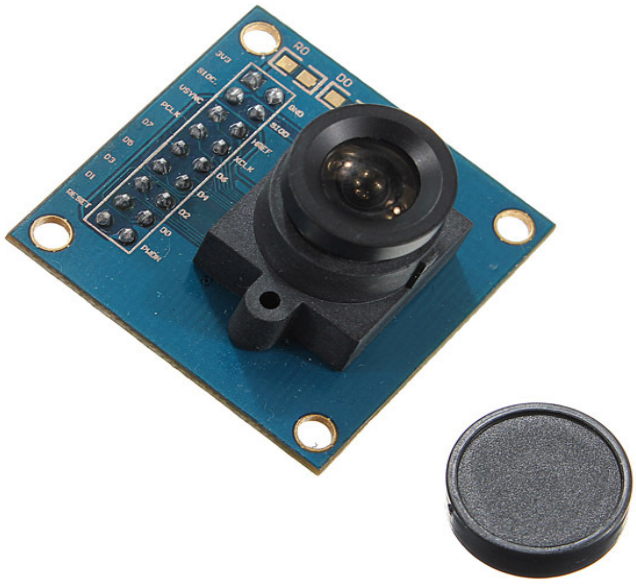


Figure 4-4 Ov7670

Specifications:

- Photosensitive Array: 640 x 480
- IO Voltage: 2.5V to 3.0V
- Operating Power: 60mW/15fpsVGAYUV
- Sleeping Mode: <20µA
- Operating Temperature: -30 to 70 deg C
- Output Format: YUV/YCbCr4:2:2 RGB565/555/444 GRB4:2:2 Raw RGB Data (8 digit)
- Lens Size: 1/6"
- Vision Angle: 25 degree
- Max. Frame Rate: 30fps VGA
- Sensitivity: 1.3V / (Lux-sec)
- Signal to Noise Ratio: 46 dB
- Dynamic Range: 52 dB

- Browse Mode: By row
- Electronic Exposure: 1 to 510 row
- Pixel Coverage: 3.6μm x 3.6μm
- Duck Current:: 12 mV/s at 60℃
- PCB Size (L x W): Approx. 1.4 x 1.4 inch / 3.5 x 3.5 cm.

Features of camera:

- High sensitivity for low-light operation
- Low operating voltage for embedded application
- Standard SCCB interface compatible with I2C interface
- With AL422 3M-Bits FIFO
- Raw RGB, RGB (GRB4:2:2, RGB565/555/444),YUV(4:2:2) and YCbCr(4:2:2)output format
- Support VGA, CIF and from CIF to 40 x 30 format
- Vario Pixel method for sub-sampling
- Auto Image Control: AEC, AGC, AWB, ABF, ABLC
- Image Quality Control: Color saturation, hue, gamma, sharpness and anti-blooming
- ISP includes noise reduction and defect correction
- Support image scaling
- Lens shading correction
- Flicker 50/60Hz auto detection
- Color saturation level auto adjust
- Edge enhancement level auto adjust
- De-noise level auto adjust

(ii) Laser and Lenses:

A simple and cheap laser source is used for the purpose of our project to make it more economical and also the user friendly because the previously proposed laser was so expensive and was hard to use by the user. A comparison is given below.

Laser	**Cost**	**Availability**	**Power**

			Supply
HRP 0500	850 Dollars	Have to be shipped from America	Used its own power supp

			l y .
5 v l a s e r u s e d	2 5 0 r u p e e s s	Read ily avail able in Paki stan	N e e d s o n l y 5 v o l t s o f D C .

Table 4-1 Comparison of PUF module with the standard PUF

Specifications:

- Output Power: 2-5mW
- Wavelength: 650nm
- Working Voltage: 5v
- Laser Shape: Dot
- Working temperature: -10℃ to +40℃
- Lens & housing: Plastic with Metal Cover
- Ready to go no other circuit required
- Dimensions: 6 X 10 mm

(iii) Arduino Uno Board:

The Arduino Uno is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an ADC adapter or battery to get started

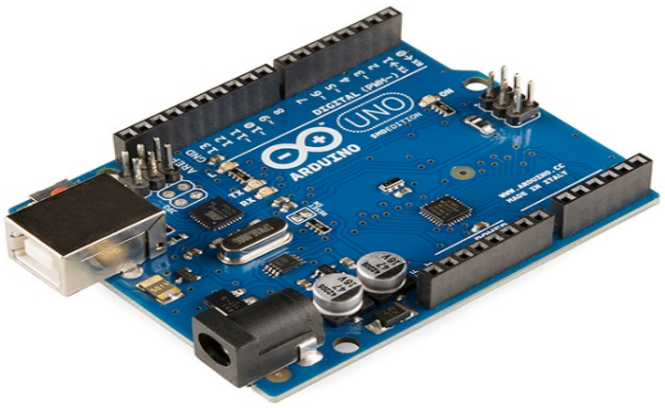


Figure4-5 Arduino Uno.

4.1.3 Motion Sensor:

Motion sensors are the devices that are used to detect and measure any motion caused in the device. They mainly consist of Accelerometer and Gyroscope. Accelerometer measures any non-gravitational motion of the device. It basically consists of microscopic crystals with give output in voltage once they sense vibration due to motion while Gyroscope gives output once it senses any rotational motion with respect to Earth's gravitational motion.

Flow Diagram:

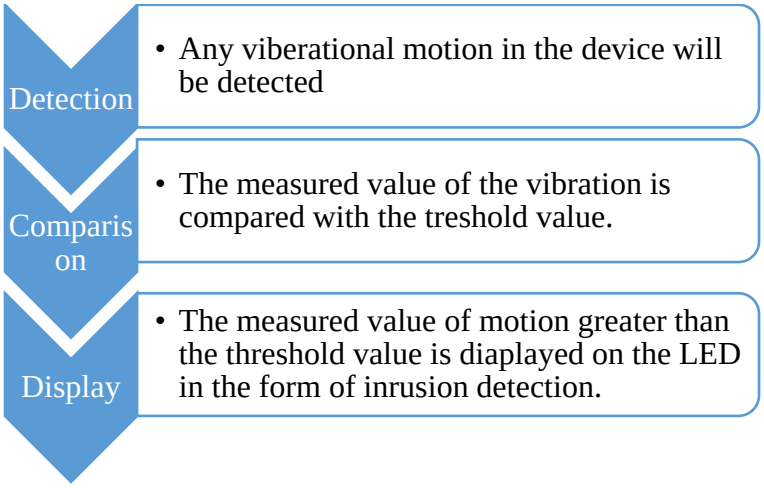


Figure 4-6 Work Flow of motion sensors

Implementation:

Motion sensor used in our project is ADXL 335 interfaced on GY 521 (MPU 6050) accelerometer.GY 521 gives output in 3 axis of rotation relative to gravitational field of force with a range of -3g to + 3g [4]. The project deals with the both accelerometer module of the device. The output of the accelerometer is interfaced with ATMEGA 32 [5] with I2C interface in which ATMEGA32 acts as master while accelerometer is acting as slave mode [6]. The address of 0x68 is stored in TWDR register of microcontroller.

Bit rate for i2c is calculated as:

Bitrate= F_CPU/ (2(TWBR) +16)

The required value of bitrate is stored in TWBR register. The bitrate requirement for MPU 6050 accelerometer can be any range between 4Hz to 1000Hz. In our project, the range sensitivity used for MPU6050 is -2g to +2g. To achieve this ATMEGA 32 is coded with AFS_SEL pin with for gyroscope. It is stored in TWCR register along with type of data to be stored. It is 0 for write control and 1 for read control.

ATMEGA 32 also deals with other two interrupts which are from external push button and pressure sensors. ATMEGA 32 is later interfaced directly with FPGA using simple digital input o FPGA.

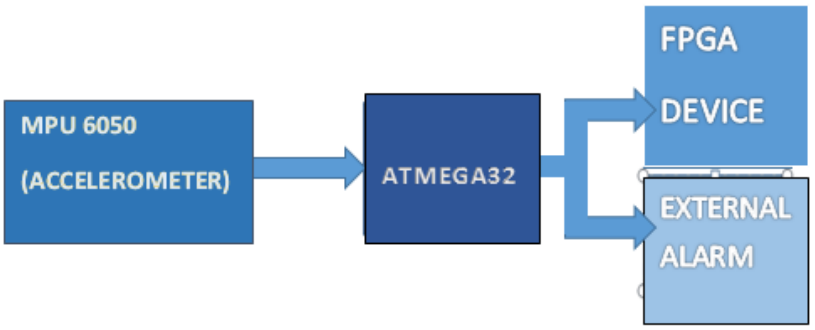


Figure 4-7 Basic Block Diagram of Motion Sensor

4.1.4 Password Protection

The password protection is being provided using Arduino board for the time being in which four users are allowed to access the device on the basis of correct password. We also tried to implement the password protection directly connecting the keyboard on FPGA but due to sensitivity issues we could not do it. The codes for FPGA are also given in appendix-B

4.1.5 Screw Protection:

The casing of the devices is protected by this module of the design. The system is activated at low level signal using IC 1404. The output of the system is interfaced to microcontroller ATMEGA 32. The input of the system is connected to the push buttons which are adjusted in such a way to give to give high level signal as long as screws are in contact with them.

Flow Diagram

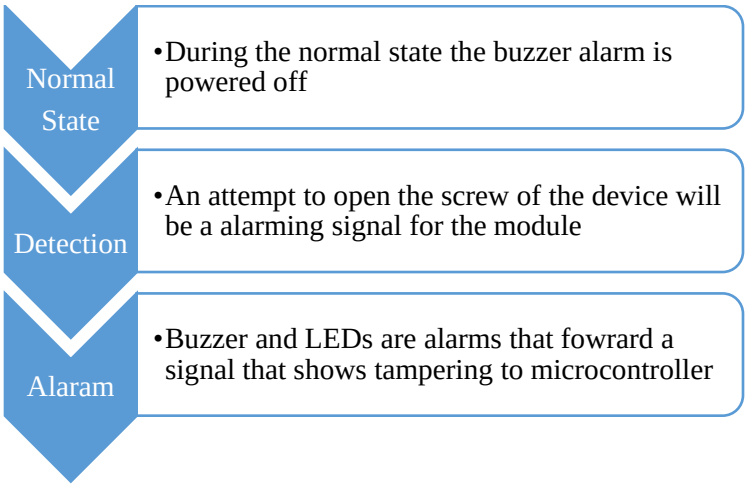


Figure 4-8 Basic Block Diagram of Motion Sensor

4.2 Hardware Requirements:

4.2.1 Biometric Based Authorization:

- R305 finger print scanner
- Arduino UNO board
- Liquid Crystal Display
- Personal computer
- Capacitors
- Push button

- Pull down resistor

4.2.2 Optical Based Authorization:

- HRP 050
- 5v laser used
- Arduino UNO board
- camera ov7670

4.2.3 Screw Protection:

- LEDs
- Buzzer Alarm
- Screw Holders

4.2.4 Motion Sensor

- MPU 6050 accelerometer
- Breadboard
- USB ASP programmer

4.2.5 Password Protection

- Arduino UNO board
- Keypad

CHAPTER 5: ANALYSIS AND EVALUATION:

Various techniques were studied and analyzed for each module of the project. However, after complete research and testing only the best possible suitable technique was selected

5.1 Biometric Based Authorization:

Various biometric technologies were considered. After a close research finger print technology was selected.

Characteristics	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Easy of Use	high	high	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signature	Noise, colds
Accuracy	High	High	Very high	Very high	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	high
Long Term Stability	High	Medium	high	high	Medium	Medium	Medium

Table 5-1 Comparison of various biometric based technologies considered

After this selection the next selection was an optimal technology for the process of finger print identification.

Technology under consideration	**Pros**	**Cons**
DSP based authorization	Had a potential for transforming into iris based identification in future.	Complexity of device increased to a level such that it was very difficult to form a communication between FPGA

		and DSP processor
SDK based authorization	A better GUI and compact device could have provided at the user	Scanners that are available in market posses a high level of encryption security.
Processor based authorization	Cost effective and relatively simple technology	Components are wide spread

Table 5-2 Comparison of technologies considered for biometric based authorization module

The results after implementation of this technology are presented here:

Enrollment is successfully achieved

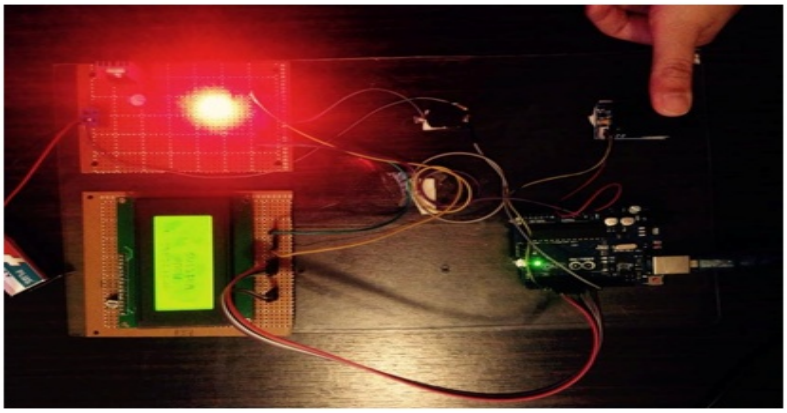


Figure 5-1 Enrollment of Finger Print

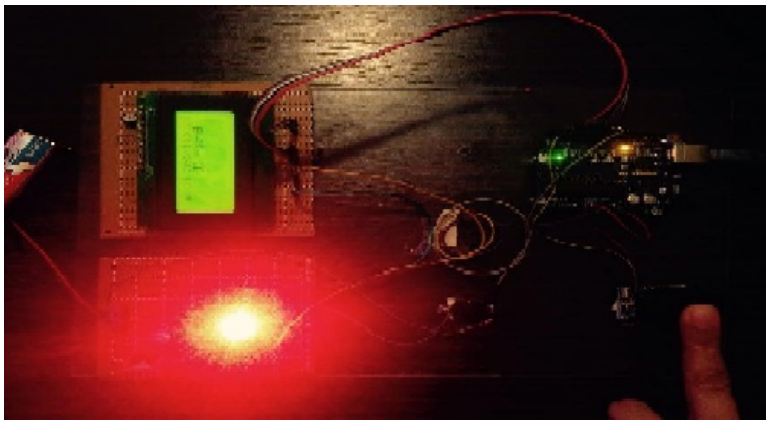


Figure 5-2 Verification of Finger Print

5.2 Optic Based Authorization:

Various techniques were considered for this module. Here is a comparison and contrast presented:

Integrated PUF	**Non-integrated PUF**
Moveable	Non moveable
Non cost efficient	Cost efficient
Hardware integration difficult	Hardware implementation easier

Table 5-3 Comparison of technologies considered for biometric based authorization module

5.3 Motion Sensor:

There were two technologies considered for this module.

MPU 6050	**MMA (3-axis)**
More reliable	Less reliable
More Efficient	Less Efficient
Difficult to interface	Easier to Interface

Table 5-4 Comparison of technologies considered for motion sensor module

Here are results attached for this module

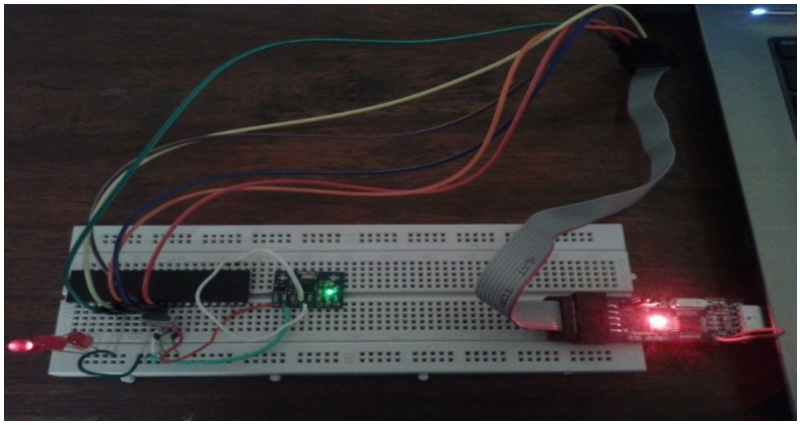


Figure 5-3 Testing of Motion Sensor

5.4Interfacing:

Some modules of this project are interfaced with ATMEGA 32 which are later interfaced with FPGA. This includes the input from the biometric identification system, screw protection system and motion sensors. An input from the pin recognizer is also fed to the microcontroller. This controller is later interfaced with FPGA. The signal that is forwarded from this controller is a proof that the device is tampered and necessary action must be taken to ensure the security of the device.

During the hardware interfacing phase, all the individual modules are brought together and secured inside the device. This required redesigning the original device and readjusting the components in the space available. An additional power supply was procured in the device to meet the requirements of the module. A backup battery is also provided inside to meet the requirement of the modules that require a constant power supply.

The codes for interfacing at the controller have been attached in APPENDIX B.

CHAPTER 6: RECOMMENDATIONS FOR FUTURE WORK:

This device will have a potential for work in order to upgrade it to level 4 of FIPS 140-2 standard by NIST. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments. Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses.

Another Future consideration could be using PUF as a method for key storage and identification. The token has a potential to store the key in itself and work on the basis of random number generator, which saves the memory and the processing.

CHAPTR 7: CONCLUSION:

7.1 Overview:

This project deals with mechanisms that serve for the purpose of tamper detection for the device. After implementation of these modules, the device meets the standards of FIPS 140-2 by NIST. For the purpose of authorization biometric based scanning and optical based authorizations have been used. These modules meet the requirements of level 2 for FIPS 140-2. For the purpose of detection, motion sensors and screw protection modules have been implemented that confront level 3 of FIPS 140-2 standard. An additional password protection module is also implemented that meets the demands of level 1, FIPS 140-2. An additional module internal to FPGA for device ID identification has also been implemented.

7.2 Objectives Achieved:

Authorization modules to meet level 2 of FIPS 140-2 by NIST have been successfully embedded inside the device. For detection purpose all the modules implemented meet the standards set by FIPS 140-2. Overall, this device meets the requirements of level 3 security standard set by NIST in FIPS 140-2

7.3 Contribution:

After implementation of these modules the device meets the standard of NIST certified device. It provides a highly secure design meeting the requirements of FIPS 140-2.

7.4 Limitations:

This device meets the level 3 security. It does not provide detection of increased temperature or voltage. Protection at such a level deals with level 4 of FIPS 140-2 which is considered a part of future considerations of this project

7.5 Applications:

This project serves to provide a good level of physical security required for a FPGA based system. An intruder trying to damage the device or slip away the required data will be successfully detected.

BIBLOGRAPHY:

[1] National Institute of Standards and Technology,“FIPS publication 140-2”, 2001, pp 1-4,15-18

[2] SasanKhosro, “DESIGN AND EVALUATION OF FPGA-BASED HYBRID PHYSICALLY UNCLONABLE FUNCTION”, 2013, pp 4-8

[3] Muneeb Mirza, “Vulnerabilities in biometric authentication and their countermeasures: A secure and efficient authentication system”, Volume 3, Issue 2, June 2014

[4] Inven Sense, “MPU 6000/MPU 6050 Product Specifications”, Revision 3.2, 11 june2011

[5] Atmel, “8-bit AVR Microcontroller with 32Kbytes In-System Programmable Flash”, February 2011

[6] Muhammad Ali Mazidi, SarmadNaimi, SepehrNaimi, “AVR MICROCONROLLER AND EMBEDDED SYSTEMS”, 2009,pp 629-642

[7] XILINX, “Developing Tamper Resistant Designs with Xilinx Virtex-6 and 7 Series FPGAs”, v (1.3), 15 October 2013, pp 9-10

[8] Arduino microcontroller Guide, ver. 2011

[9] Finger Print Module Specification by Aratek biometrics technology Co. Ltd

APPENDIX A

Extended Title:

Developing tamper evidence (detection) techniques with Xylinx Vertix-6 and Vertix-7 series FPGA.

Brief Description of The Project / Thesis with Salient Specs:

Tamper detection is the ability to make the system or user aware of the tamper event. In FPGAs, programming failures caused by not using the correct AES key may indicate a tamper event. On a system level, an attempt to open up a system box or casing may indicate a tamper event.

Scope of Work:

This is a company based project titled: Trusted Computing on FPGA based system. It is divided into two modules. One module covers detection of key tampering and other module will erase the encryption key if any tampering is detected in BBROM. We will be working with the module of detection of key tampering from the ROM.

Academic Objectives :

After the compilation of this project we will be skilled at Verilog programming, including FPGA structures and working on vertex-6.This is a project sponsored by NESCOM to be utilized by the industry after its completion.

Application / End Goal Objectives :

To provide security to the data stored in FPGA Flash ROM.Any attempt of tamper will be detected by the code and hardware implemented by us.

This project has a general approach. Any device working with FPGA can be secured by this.

Previous Work Done on The Subject :

Xylinx itself provides tampering resistance and techniques for FPGA.Tamper detection has been implemented in vertex 5.Links for

vertex 5 tamper detection/resistance techniques and books for such techniques are given below.

- http://www.rsaconference.com/writable/presentations/file_upload/cryp-107.pdf
- http://books.google.com.pk/books?id=J3ERJHJ_QuEC&pg=PA15&lpg=PA15&dq=tamper+resistance+in+xilinx+virtex+5&source=bl&ots=_RpQN47cle&sig=ZKXq4c2cKW1fBRx0u_s_hWQH5iw&hl=en&sa=X&ei=m7EuU4TvNdOB7Qb-kYCoBg&ved=0CG4Q6AEwCA#v=onepage&q=tamper%20resistance%20in%20xilinx%20virtex%205&f=false
- Solving Today's Design Security Concerns
  By: Ching Hu
- On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks
  – Extracting Keys from Xilinx Vertix-II FPGAs –

Material Resources Required:

FPGA (XYLINX) kit vertex-6 kits (3 in number), PC systems (3 in number), BBRAM (3 in number), LEDS, Data Cables (3 in number), Monitoring Alarms.

All Equipment to be provided by NESCOM.

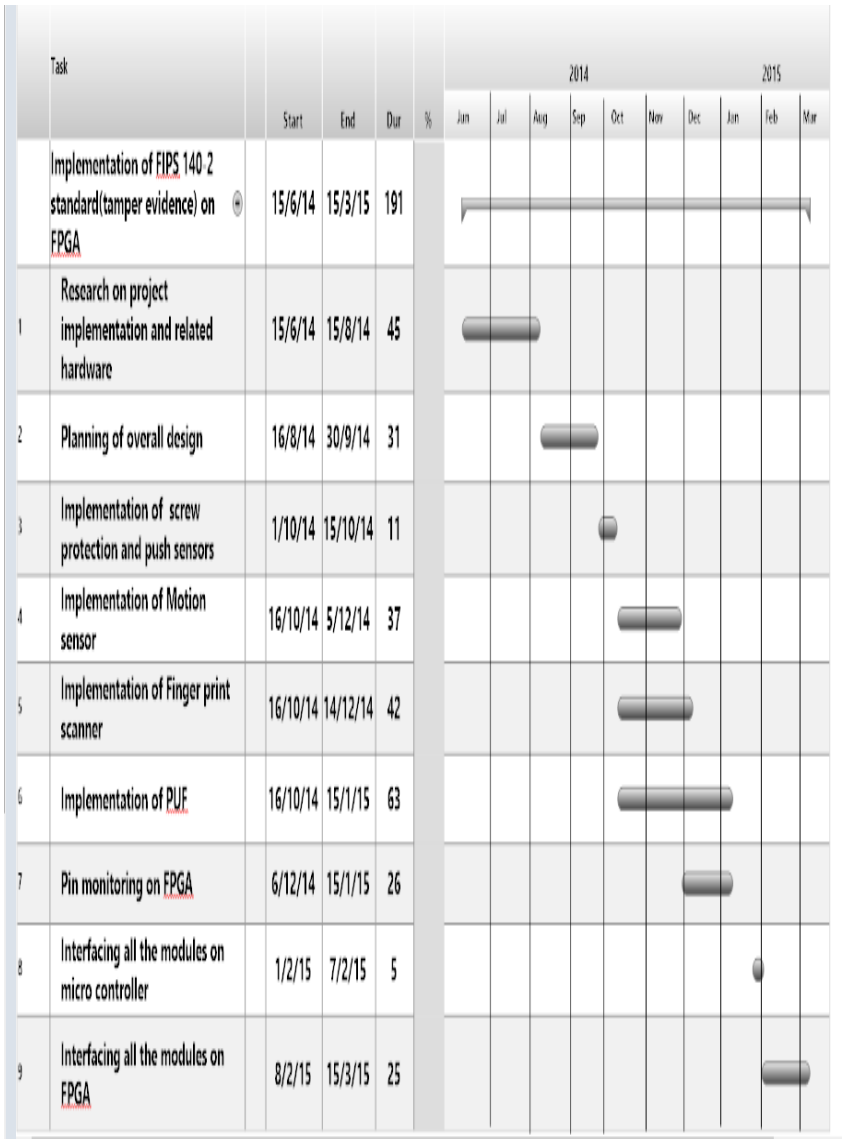
No of Students Required :3

Special Skills Required:

Verilog/VHDL programming and understanding of FPGA. Understanding of cryptography and encryption and decryption of data stored through keys. Knowledge of FIPS standards for encryption of data.

APPENDIX B

TIMELINE FOR THE PROJECT



	Task	Start	End	Dur	%
	Implementation of FIPS 140-2 standard(tamper evidence) on FPGA	15/6/14	15/3/15	191	
1	Research on project implementation and related hardware	15/6/14	15/8/14	45	
2	Planning of overall design	16/8/14	30/9/14	31	
3	Implementation of screw protection and push sensors	1/10/14	15/10/14	11	
4	Implementation of Motion sensor	16/10/14	5/12/14	37	
5	Implementation of Finger print scanner	16/10/14	14/12/14	42	
6	Implementation of PUF	16/10/14	15/1/15	63	
7	Pin monitoring on FPGA	6/12/14	15/1/15	26	
8	Interfacing all the modules on micro controller	1/2/15	7/2/15	5	
9	Interfacing all the modules on FPGA	8/2/15	15/3/15	25	

APPENDIX C

Cost Break down:

Component	Quantity	Vendor's information	Cost per item(Rs /-)
Finger print sensor R305	2	LLIED Allied Electronics	7200/-
16 x 4 LCD	1	LLIED Allied Electronics	1000/-
Arduino UNO	2	LLIED Allied Electronics	2700/-
Vero Board	1	LLIED Allied Electronics	2000/-
Finger print sensor GT-511-C3	1	LLIED Allied Electronics	6000/-
Finger print scanner (used)	1	Mr. Computer	1000/-
u.are.u 4500	1	Digital persona	9000/-
Other components (battery,heatsink, wires,capacitors,	-	Dynamo Electronics	500/-

etc)			
MPU 6050 accelerometer	1	IC Master	500/-
USB ASP programmer	1	IC master	800/-
Acrylic Sheet	1	Plastic Store	2000/-
Lenses	2	Sohail Science Store	500/-
Laser	4	EBS electronics	500/-
Voltage supply adopter	1	IC Master	200/-
Key Pad	1	Oceana Electronics	100/-
Switches	10	Oceana Electronics	500/-
Lose wires	50+	IC Master	1000/-

Miscellaneous	-	IC Master	2000/-