Sri Lanka Institute of Information Technology

RESEARCH PROPOSAL

Portable Solution for High Secure Encryption of Removable Storage Media

Author:

Tharindu Piyasekara

MS13961336

Supervisor:

Lakmal Rupasinghe

Senior Lecturer

SLIIT

MSc Research Project

Department of Information Technology

July 2014

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Abstract

Faculty of Computing

Department of Information Technology

MSc in IT (Specialization: Cyber Security)

Portable Solution for High Secure Encryption of Removable Storage Media

by Tharindu Piyasekara MS13961336

Although there are cryptographic solutions already developed for data encryption purposes, there are situations where the removable data storage devices cannot be encrypted or decrypted as the required sources are not available. And the existing solutions need an application installed in a computer to encrypt the device. Nowadays the users are always looking for small potable solutions to make their lives easier. Since the existing solutions are not sufficient enough to fulfill their requirements. This is one of the major reasons that cause data leakages outside of an organization. Goal of the research study is to decrease the data leakage due to the unencrypted removable data. Developing a portable cryptographic solution to secure the data stored in the removable data storage devices and improving performance and user-friendliness of the solution are the main objectives which support to achieve the goal of this research project. Proposed research will follow the deductive methodology and will use quantitative approaches to collect data. Analyzed data is used to compare with the existing solutions to improve and validate the successfulness of the research. Expected outcome of the research is a device so called Crypto-Hub. Crypto-Hub will be important to fulfill the gaps in the information based world in order to secure the data stored in removable USB and MTP supported storage media.

Contents

List of Figures

Abbreviations

BYOD	**B**ring **Y**our **O**wn **D**evice
IT	**I**nformation **T**echnologyr
MTP	**M**edia **T**ransport **P**rotocol
OS	**O**perating **S**ystem
USB	**U**niversal **S**erial **B**us

Chapter 1

Project Description

1.1 Introduction

The field of information security has evolved and grown significantly in recent years. IT security specialists have stated that there is a high value for information within a large scale organization as well as in an individual person's life. It is said that it is necessary to keep all the technologies within the company secure from malicious cyber-attacks that often attempt to breach private and sensitive information or gain control of the internal systems. The average cost of a data breach from any source ranges from $100,000 to $2.5 million.

Removable media ease the transferring of data for storage and business purposes in day-today life. USB and Media Transport Protocol (MTP) supported devices (e.g. thumb drive, MP3 player, camera, smart phone, portable hard disks etc.) have become important devices which interact with the computer. Information security plays a major role in this scenario as the removable media are also being used to transmit secured data. Cryptography, access controlling mechanisms and information classification techniques are used to ensure the security of sensitive information within an organization.

BYOD is now common in organizations; those devices can be personal computers, mobile phones, and other data storage devices. This adds more challenges to the

removable device data security. According to the industrial expertise, surveys carried out in different organizations and also the other researchers who have done researches on information security domain have mentioned that the external removable devices owned by the organization and personal devices do not possess the same level of security that the organization information possesses internally. The level of security of the information or the data extracted from a particular organization is poor compared to the data when inside the organization. A SanDisk survey shows 25% of data corporate end users most frequently copy customer data. Organizations have the full responsibility of customer data after collecting the data from the customer. Most of the time, the auditors and the policy developers forget and do not care much about these kinds of scenarios and because of that, the security level of removable devices are poor compared to the security level in the internal systems. Due to this reason, the removable devices have become weak linkers and easily attackable points as well as a common vulnerability in information security.

1.2 Problem Statement

In cryptography, a Caesar cipher, which is also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known and used encryption techniques. It indicates and proves that the information security is not just a brand new problem which suddenly arose in this century but was an issue from a quite long time. The researchers were able to overcome those problems for some extent providing various types of solutions. The field of information security has grown and expanded significantly during last few years with the modern technology. The researchers are already working on the researches based on security issues and the currently available solutions are capable of addressing some of the security issues only. In this chapter the existing ideas, alternatives considered in this problem are discussed.

Since this security problem is not solved completely, many researchers are carrying out various types of researches to fulfil the gap. Some expertise says that the security of the physical drives cannot be guaranteed without compromising the benefits of portability. But there are some alternative solutions addressing this problem. As I identified, there are mainly two types of researches carrying out on this area.

- Encryption applications developed to run on computers
- Encrypted secure drives

1.2.1 Encryption Applications Developed To Run On Computers

Using this sort of encryption software is the most common way to secure the data in the removable storage media. In here, the particular software has to be installed on a computer and the user needs to plug the device into the computer and carry out the process of encryption to secure the data. But the limitation is that this application might change from OS to OS since those applications have different flavours for different OSs. The encryption algorithms are used here to secure the data. Encrypted data can be copied into the removable storage device. Whenever the user needs to make use of the encrypted data, the device has to be plugged into the computer and should follow the process of decrypting.

E.g.: Trucrpt, BitLocker (formerly BitLocker Drive Encryption)

Even though there is a warning that using TrueCrypt is not secure, Trucrpt is top rank software among the other encryption software available. Trucrpt has different versions for Windows, Linux and Mac OS separately. And BitLocker is a full disk encrypting feature included with the Windows OS. It is designed to protect data by providing encryption for entire volume.

1.2.2 Encrypted Secure Drives

These devices are self-encrypted devices. After coping data into these devices, the data will be automatically encrypted. Whenever the user needs to use the encrypted data, the user will simply have to plug the device into computer and decrypt the data. Some of these solutions have certifications and some of the devices having their own algorithm do not have certifications. Normal portable storage devices cannot be converted into encrypted secure drives and these devices are specially designed for the purpose of securing data and such devices are highly expensive compared to the price of the normal removable storage devices.

E.g. Data Traveler Vault devices developed by Kingston, devices developed by Rohde & Schwarz SIT

Above mentioned solutions have pros and cons. The Figure 1.1 contains a discussion of alternatives solutions. As mentioned in the table those two products have Pros and Cons. And none of it fulfils the required gap of the research problem.

	Encryption applications developed for run on computers	Encrypted secure drives
Confidentiality	Moderate	Moderate
Integrity	Moderate	Moderate
Availability	Low	High
Cost	Cost is low	Cost is high
User Friendliness	Can't use sure data without a computer or opening a laptop	Normal device user need buy new devices
Encryption mechanism	Cryptography (Hardware/Software)	Cryptography (Software)
Suitable level	This can be use for any size of organization	Most suitable for large size organization.
Usability	Need to install on computers	Current devices cannot be use for this

FIGURE 1.1: Existing Solution

1.3 Research Questions & Research Objectives

1.3.1 Research Question

The information leakages occurring due to the unsecured removable devices have become one of the major threats to the field of information security. Although there are cryptographic solutions already developed for data encryption purposes, there are situations where the removable devices cannot be encrypted or decrypted as the required sources are not available such as when the user is travelling. This is because when there is a need of encrypting or decrypting data in a removable device, it has to be plugged in to a computer in which a particular data protection application is already installed to carry out with the process of cryptography.

User requirement is to have a user-friendly and an easy method to secure data. And on other hand the security professional's purpose is to make sure that the data is secured after applying cryptographic mechanisms to data. The problem is to provide a better solution for this and to make sure that the solution fulfils both the requirements. Otherwise it is not going to be a good solution to this problem. The research question is how to provide a user-friendly and a trust-worthy and secured solution for the removable data storages devices.

1.3.2 Research Objectives

The proposed research will be carried out for the purpose of identifying the user requirements and accept the security level of the removable devices and to design and develop a portable cryptographic solution to secure the data in the removable devices. This would be a fast and handy solution with a portable device. Proposed device is small in size, user-friendly and the ideal solution to address and respond the current issues in data leakage occurs due to unsecured removable devices in an effective manner.

Main objective:

- The main objective of this research project is to find out a solution for data leakage taking place due to transferring and storing data in unsecured removable data storage devices.

The main objective is split up into following four specific objectives:

1. Designing a specific low cost device to encrypt the data stored in the removable storage media.
   Encrypting data in the removable storage devices is not considered as a very important matter even in organizational level. But it is very important to protect the sensitive data specially when taken out of an organization for different purposes. The proposed device is capable of encrypting and decrypting data in the removable storage media in the absence of a typical computer.

2. Identifying the user requirements and creating a handy device
   The proposed device with the cryptography mechanisms will be a user friendly device which is small in size and light-weighted where the user is able to carry it whenever necessary. Also the requirements gap will be identified and filled using a survey.

3. Developing a device that possess a high durability
   The life time of the device depends on the durability of the battery. The proposed device will possess a quite sound life time and hence the user will be provided with a device which has a high durability compared to the other battery powered devices.

4. Analysing the processes and decreasing the time consumption for encrypting.
   The proposed application has to be more efficient so that the user will find it easier to encrypt the data as they wish and would not waste time.

1.4 Hypothesis

If there is a portable high secured device which can be used to secure the data stored in the removable storage devices, the data leakage occurs during transferring and storing data using unsecured removable data storage devices can be minimized.

1.5 Methodology

Proposed research will follow a deductive methodology. This research uses existing theories on data encryption research domain and new experiments to find out the new facts. Objectives are clearly defined in this research but research problem is not directly defined. The proposal is to design and develop a solution and to find out a better solution for the research problems. In this research, accessing and using some parts of the research is already being completed in the cryptography domain. This project consists of two main sections. One is developing the proposed solution and the other is collecting data to determine the success of the research. By considering the nature of this research this will be conducted as a structured exploratory applied research. The next section describes more about data collection.

Figure 1.2 shows the areas considering when designing the device which can be used to secure the removable data storage devices.

Single board computers will be used as the device and it is powered by a battery and will be modified in such a way it can be used to encrypt and decrypt the data in portable storage devices. Linux based OS will run on top of this device and also the device will consist of an interface to commutate with the user. This device will be known as Crypto-Hub. User can plug the removable device in to the Crypto-Hub and carry out encryption and decryption processes. Crypto-Hub encrypts the data in the storage device which is plugged to the computer so that the data is encrypted and the user will not have to worry about the security of the data in the

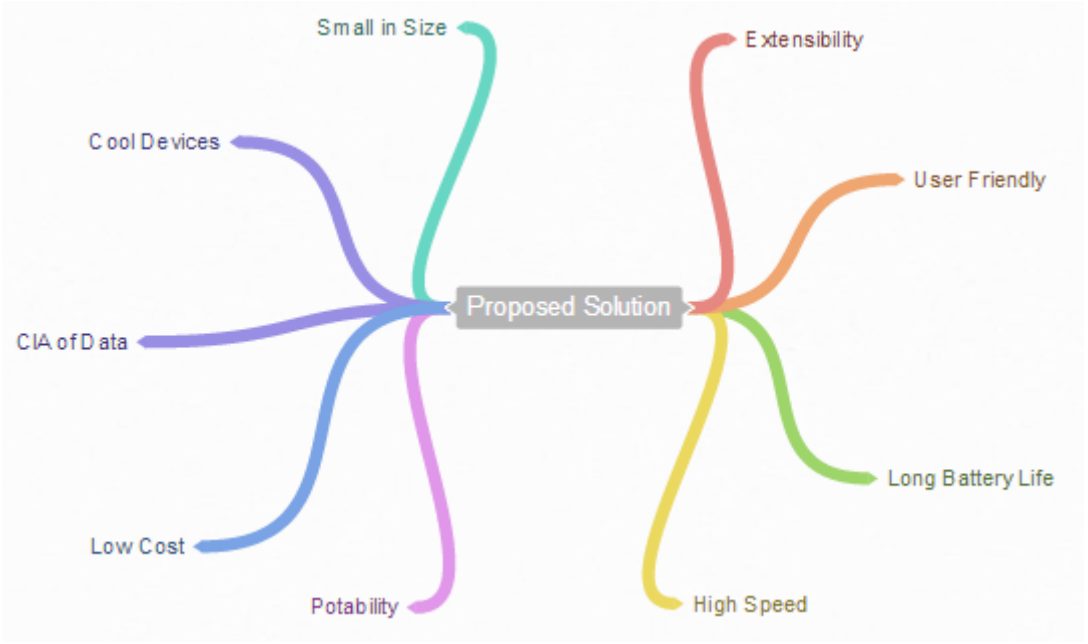

FIGURE 1.2: Proposed Solution Outline

removable device and that could be carried anywhere the user goes with no harm to the data. The user has to plug the removable device back to the Crypto-Hub and decrypt the encrypted data to make use of the data in the removable devices. User is provided with different security levels and is allowed to select the options preferred according to the requirement. The two factor authentications will be used for the process of encryption. The password has to be provided by the user and the device will validate the removable device before the process of encryption, making it a trust worthy, reliable and a more secure encryption mechanism to encrypt the data in removable devices. In a case if the user is unable to provide the password the user will be provided with an alternative way to decrypt the encrypted data.

As described above once this research study achieves the above stated objectives, potential outcome will be portable encryption devices which can be used to reduce the data leakages take place due to unsecured removable data storage devices. This device is a user-friendly and a low cost device with high level cryptographic algorithms.

1.6 Data Collection

1.6.1 Data

Proposed research study will follow the deductive methodology and will use quantitative approaches to collect data such as the level of security, speed, size, and also the user requirements and user satisfaction. Analysand data are used to compare with the existing solutions to improve and validate the successfulness of the research. And mainly depends on the primary data. Primary data is used to measure the effectiveness of the solution and secondary data is used to identify where the issue is and the direction of the research.

After completing the development part of the solution, the performance and other qualitative measurement details have to be considered to measure the effectiveness and the efficiency of the proposed solution. Below table shows the primary data collection methods for the research.

Data	Data Collection Methods
Time taken for encrypt a file	Observations
Size of the devise	
Durability of the device battery life	
User-friendliness	Interviews and questionnaires

FIGURE 1.3: Data Collection Methods

Company records or archives, government publications, industry analysis offered by the media, websites etc. will be used as secondary data collection methods in this project.

1.6.2 Data Analysing

Analysing the collected information plays an important role in this project. Data collected by the observations, interviews and questionnaires are needed to be combined together to find out the relationships in between those variables and what is the impact for the final objective of the research.

1.6.3 Data Evaluation

After analysing those collected variable values, the next step is evaluating those data. Main task is to identify the relationship/s between level of security, speed, size, and also the user satisfaction. Some variable values will be modified in this case in order to identify the correct relationships between variables and to find out the best solution for the problem.

1.6.4 Ethics in Data Collection

The information given by an organization and a particular individual is treated highly confidential. Each entity is treated as atomistic entity and there will be no comparison done with the given information of another entity. Individual or organization is not relevant to the objectives of this study. These are convinced to the respondent prior to the request for information.

1.7 Working Plan & Time Schedule

Figure 1.4 shows the project plan of the proposed research project. Starting date of the project development will be on 1st of August 2014 and have planned to complete research study and publish the outcome by 1st of December 2014. The literature reviewing and feasibility studying has been successfully completed within a period of two months before starting the development process of the project. There are six main tasks to be completed within time duration of four months.

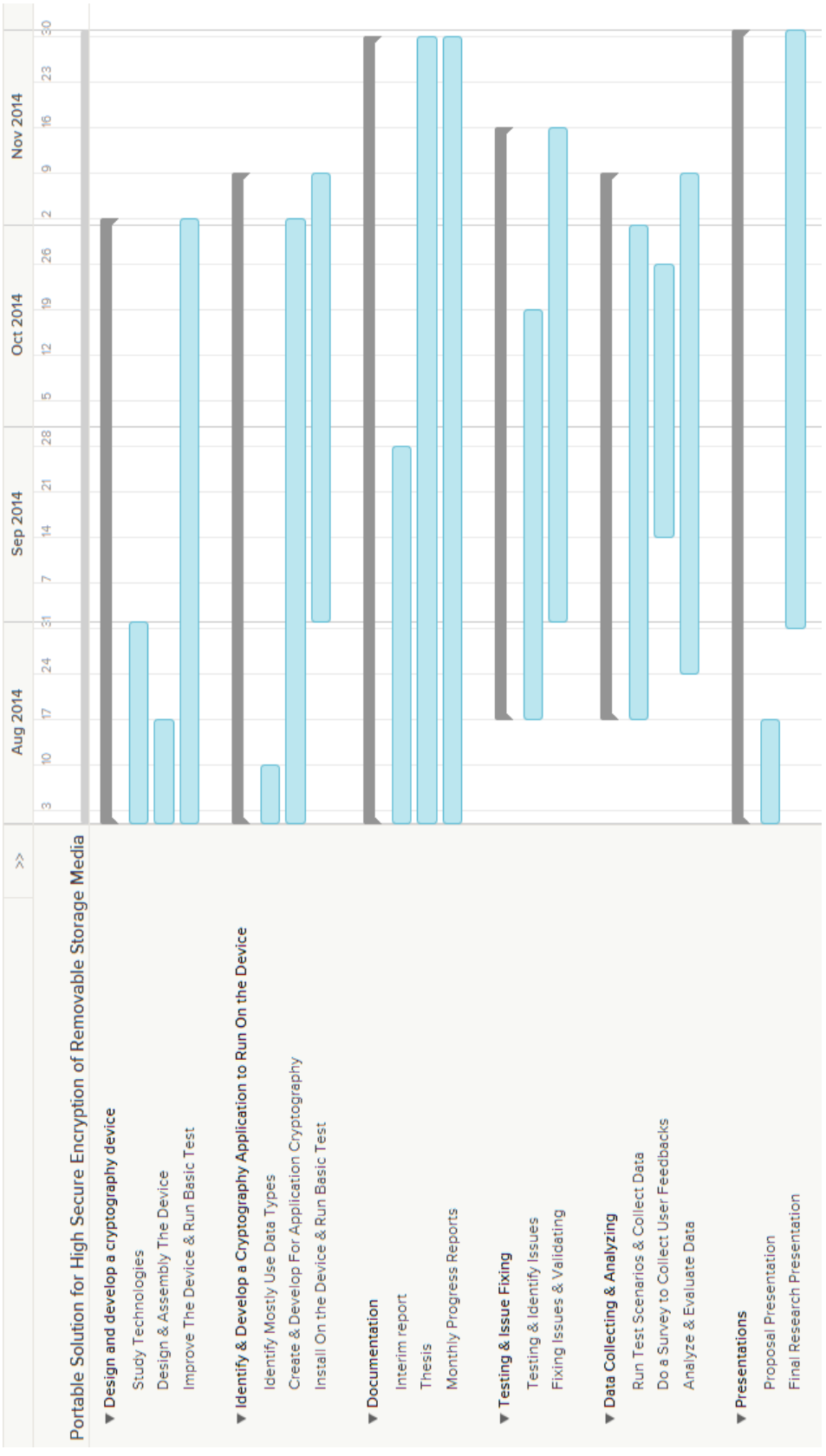

FIGURE 1.4: Project Plan

1. Designing and developing the devices
2. Identify and developing the cryptographic application to run the device
3. Documentation
4. Testing and issue fixing
5. Data collecting and analyzing
6. Presentations

1.8 Facilities Required

It is necessary to have the guidance of the project supervisor, module coordinator and other course related resource persons to complete the research project as well as the course successfully. And also it would be better to have the opportunity to contact resource persons from the engineering department in a case if there are things to get clarified regarding electronics. Guidance and the support given by the institute throughout the project development process would be highly appreciated.

1.9 Feasibility

The field of information security is moving towards the goal of implementing secured cyber system. Fulfilling security requirement as soon as possible is important. The outcome of the project feasibility study would be described in this chapter. Estimated time duration for this research study is four months. Research study and the given time duration has identified as most challenge areas to the project. The study includes three major stages. First stage is studying the groundwork, then the information gathering and finally the presentations and thesis. Figure 1.5 shows the results of the feasibility study. (Cannot done = 1, Can successful = 10)

Stages	Sub Area	Result
Study groundwork	Accessibility of technologies & knowledge required for research works	9
	User requirement	10
	Project Budget	10
	Time line	9
	Funding resource	10
Information gathering	Resource available to collect information	10
	Validity of information	10
Presentations & Thesis	Data analyzing and reporting	10
	Course requirement	10
	Thesis	10

FIGURE 1.5: Result of Feasibility Study

Chapter 2

Budget

Estimated total budget to undertake the research study successfully is Rs. 78320.00. This includes the cost of developing and testing the device, publication cost and an additional 10% overhead. Expenditures are allocated for an extra Raspberry-pi board in a case if necessary but will not be necessary at the beginning of the project. Funding sources for the research study are welcome, but if unable to find a funding source, the budget would be handled of my own. And the research project expenses will be covered by introducing the product to the preferred investor/s once the project is successfully completed.

Budget

Budget Item		Amount (Rs)	Sub-Total(Rs)
Deluxe Raspberry Pi Starter Kit			
	Deluxe Raspberry Pi Starter Kit	27,600.00	
	Shipping + Tax	9,500.00	
Totale expecess for Deluxe Raspberry Pi Starter Kit expecess			37,100.00
Extra Raspberry -pi board			
	Raspberry Pi - Model B	6,400.00	
	Shipping + Tax	2,500.00	
Totale expecess for Extra Raspberry -pi board			8,900.00
Power unit			1,800.00
Reachable Batteries			4,000.00
Cost of developing a power supply unit			4,000.00
Graphic display unit			6,800.00
Cables and converters			3,500.00
2GB Pen drive (Testing perpose)			1,100.00
Cost for creating a device casing			1,000.00
Publications			
	Prining & binding the thesis	2,500.00	
	Printing other doucmnts	500.00	
Totale expecess for Publications			3,000.00
Total direct expense			**71,200.00**
Indirect costs (10% of total direct expense)			7,120.00
TOTAL PROJECT EXPENSES			**78,320.00**

FIGURE 2.1: Estimated Project Budget

Appendix A

Sketch of Proposed Devise

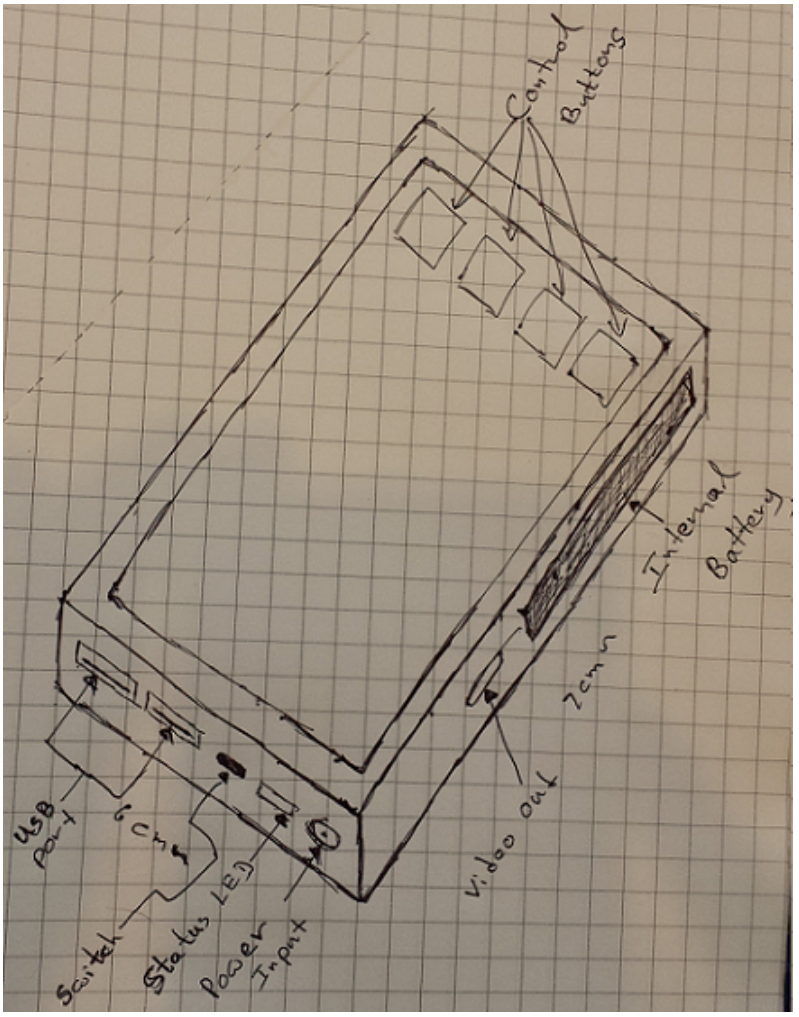

FIGURE A.1: Sketch of Proposed Devise

Bibliography

[1] Meulen R.V.D. 2013 Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes [Internet]. Gartner, STAMFORD, Conn. http://www.gartner.com/newsroom/id/2466615

[2] Tabaka, G, 2013. Haking On Demand. 2nd ed. 02-682 Warszawa, ul, Bokserska 1: Software Press Sp. Z o.o SK.

[3] Sundaram, G.S, 2013. Bluetooth communication using a touch screen interface with the Raspberry Pi. 1st ed. Jacksonville, FL: Available from:IEEE.

[4] Ferguson, N, 2006. AES CBC Elephant diffuser A Disk Encryption Algorithm for Windows Vista . 1st ed. Microsoft: Microsoft Corp.

[5] NOISE. 2012. Raspberry Photoplethysmograph. [ONLINE] Available at: http://www.noise.inf.u-szeged.hu/Instruments/raspberryplet/. [Accessed 07 June 14].

[6] SecurPassword.2014.Secur Password.[ONLINE] Available at: https://www.securenvoy.com/products/securpassword/overview.shtm.[Accessed 07 June 14].

[7] Gomes, , O.S.M. 2011, A fast cryptography pipelined hardware developed in FPGA with VHDL. Available from IEEE, [Accessed 07 June 14].

[8] Richardson, M, Wallace, S 2012. Getting Started with Raspberry Pi. 1st ed. United States of America: Maker Media, Inc.