K.ELATRESH

UNIVERSITY STUDENTS' ATTITUDES TOWARDS CAPTCHA USE

KHALID ELATRESH

ATILIM UNIVERSITY 2019

JANUARY 2019

UNIVERSITY STUDENTS' ATTITUDES TOWARDS CAPTCHA USE

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

BY

KHALID ELATRESH

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
INFORMATION TECHNOLOGY

JANUARY 2019

Approval of the Graduate School of Natural and Applied Sciences, Atilim University.

_____

Prof. Dr. Ali KARA

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of **Master of Science in Information Technology, Atilim University**.

_____

Assoc. Prof. Dr. Korhan Levent ERTÜRK

Head of Department

This is to certify that we have read the thesis UNIVERSITY STUDENTS' ATTITUDES TOWARDS CAPTCHA USE submitted by KHALID ELATRESH and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Assoc. Prof. Dr. Murat KOYUNCU

Supervisor

Examining Committee Members:

Assoc. Prof. Dr. Murat Koyuncu
Information Systems Engineering, Atilim University _____

Asst. Prof. Dr. Atila Bostan
Computer Engineering, Atilim University _____

Asst. Prof. Dr. Can Güldüren
Management Information Systems, Ufuk University _____

Date: 28 January 2019

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

KHALID ELATRESH

Signature:

ABSTRACT

UNIVERSITY STUDENTS' ATTITUDES TOWARDS CAPTCHAUSE

ELATRESH, Khalid

M.Sc, Information Technology

Supervisor: Assoc. Prof. Dr. Murat KOYUNCU

January 2019, 59 Pages

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a type of techniques that is utilized in order to be able to distinguish the actual human users from bots or for determining the users that are authorized to access a website or a file on the Internet. This thesis aims at determining attitudes of Libyan students towards different types of CAPTCHA in WWW environment. It also analyzes user attitudes according to demographic and Internet usage information including gender, age, education level, for how many years they have been using the Internet, and how often they use the Internet. To fulfill the purpose of the study, a questionnaire was prepared and Libyan students studying in different levels and departments answered to the questionnaire that is published through the Internet.

The data obtained is processed using SPSS 18.0 software package. The obtained results reflect that the participants are familiar with all of types of CAPTCHA since they use them every day through navigating in the Web for books or scientific articles. However, user familiarity for text-based CAPTCHA is higher than the others. The No CAPTCHA reCAPTCHA type is the most favored one from different perspectives including error freeness, easiness, and security. Therefore, we conclude that the No CAPTCHA reCAPTCHA type is the most preferred type by users.

Keywords: CAPTCHA, security, user attitudes, WWW

ÖZ

ÜNİVERSİTE ÖĞRENCİLERİNİN CAPTCHA'YA YÖNELİK TUTUMLARI

ELATRESH, Khalid

Yüksek Lisans, Bilgi Teknolojileri

Tez Yöneticisi: Doç. Dr. Murat KOYUNCU

Ocak 2019, 59 sayfa

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) gerçek insan kullanıcıları botlardan ayırt etmek veya bir web sitesine veya dosyaya erişim yetkisi olan kullanıcıları belirlemek için internette kullanılan bir tür tekniktir.Bu tez çalışması, Libyalı öğrencilerin WWW ortamında farklı CAPTCHA tiplerine yönelik tutumlarını belirlemeyi amaçlamaktadır. Ayrıca, cinsiyet, yaş, eğitim düzeyi, kaç yıldır İnternet'i kullandıkları ve ne sıklıkla İnternet kullandıklarını da içeren demografik ve İnternet kullanım bilgilerine göre kullanıcı tutumlarını analiz eder. Araştırmanın amacına ulaşmak için bir anket hazırlanmış ve farklı düzeylerde ve bölümlerde okuyan Libyalı öğrenciler internetten yayınlanan ankete cevap vermiştir.

Elde edilen veriler SPSS 18.0 yazılım paketi kullanılarak işlenmiştir. Sonuçlar, katılımcıların sürekli Web'de kitap ya da bilimsel makaleler bulmak için gezindikleri için CAPTCHA türlerine aşina olduklarını göstermektedir. Ancak, metin tabanlı CAPTCHA için kullanıcı aşinalığı diğerlerinden daha yüksektir. CAPTCHA reCAPTCHA tipi, hatalara karşı duyarlılık, kolaylık ve güvenlik dahil olmak üzere farklı bakış açılarından en çok öne çıkan olmuştur. Bu nedenle, CAPTCHA reCAPTCHA tipinin kullanıcılar tarafından en çok tercih edilen tip olduğu sonucuna varılmıştır.

Anahtar Kelimeler: CAPTCHA, güvenlik, kullanıcıtutumu, WWW

DEDICATION

To …My Family and Friends

ACKNOWLEDGMENTS

I would like to express my thanks to Assoc. Prof. Dr. Murat KOYUNCU for his advice and support in order to complete this research.

I shall also thank to my family for their support.

Furthermore, I thank to the members of the IT department.

Finally, I shall also thank to my friends for their help.

TABLE OF CONTENTS

ABSTRACT iii

ÖZ iv

DEDICATION v

ACKNOWLEDGMENTS vi

TABLE OF CONTENTS vii

LIST OF TABLES x

LIST OF FIGURES xi

LIST OF ABBREVIATIONS xii

CHAPTER 1 1

INTRODUCTION 1

1.1. Subject Overview 1

1.2. Study Aim and Research Questions 4

1.3. Thesis Organization 4

CHAPTER 2 5

LITERATURE REVIEW 5

2.1. Information and Communication Technology (ICT) 5

2.2. Internet Security Challenges 6

2.2.1. Lack of International Supervision 8

2.2.2. Lack of International Data Protection Standards/Legislation 8

2.2.3. Authentication/Identification Requirements 8

2.2.4. Confidentiality Requirements 9

2.2.5. Interruption of Service 9

2.2.6. Masquerading 10

2.2.7. Repudiation 10
2.3. CAPTCHA Definition and Usage 10
2.3.1. CAPTCHA Use 11
2.3.2. CAPTCHA Attacks 13
2.3.3. Types of CAPTCHA 13
2.4. Attitudes towards CAPTCHA 15
2.5. Usability of CAPTCHA 17
2.6 Alternatives to CAPTCHA 18
CHAPTER 3 20
METHODOLOGY 20
3.1. Questionnaire Design 21
3.2. Sample and Analysis 27
3.2.1. Population and Samples 27
3.2.2. Instrument 27
3.2.3. Data Collection Execution 28
3.2.4. Validity and Reliability Issues 28
3.2.5. Data Analysis Framework 28
CHAPTER 4 29
FINDINGS AND DISCUSSION 29
4.1. Descriptive Findings 29
4.1.1. Demographic Information of Participants 29
4.1.2. Students Understanding and Awareness of CAPTCHA 33
4.2. Statistical Analysis 34
4.2.1. Attitudes towards picture-based CAPTCHA 35
4.2.2. Attitudes towards text-based CAPTCHA 36
4.2.3. Attitudes towards arithmetic-based CAPTCHA 37

4.2.4. Attitudes towards No CAPTCHA reCAPTCHA 38
4.2.5. Attitudes towards game-based CAPTCHA 39
4.3. Discussion 40
CHAPTER 5 48
CONCLUSION AND RECOMMENDITION 48
5.1. Conclusion 48
5.2. Recommendation 48
REFERENCES 49
APPENDIX 54

LIST OF TABLES

TABLES

Table 4.1: Demographic Information of participants 29
Table 4.2: Descriptive statistics of these 13 questions 34
Table 4.3: Attitudes towards picture-based CAPTCHA.....35
Table 4.4: Attitudes towards text-based CAPTCHA.....36
Table 4.5: Attitudes towards arithmetic-based CAPTCHA.....37
Table 4.6: Attitudes towards No CAPTCHA reCAPTCHA 38
Table 4.7: Attitudes towards game-based CAPTCHA 39
Table 4.8: Means and standard deviations of attitudes towards different types of CAPTCHA.....40
Table 4.9: Familiarity and attitude for each kind of CAPTCHA 42
Table 4.10: The success rate for each kind of CAPTCHA 43
Table 4.11: The response time for each kind of CAPTCHA 44
Table 4.12: Attitude regarding to age 45
Table 4.13: The security preference for each kind of CAPTCHA 46

LIST OF FIGURES

FIGURES

Figure 2.1: Concept of CAPTCHA.....11
Figure 2.2: Some Examples of Text-Based CAPTCHA.....14
Figure 2.3: Some Examples of Image-Based CAPTCHA.....14
Figure 2.4: An Example of Multi-model CAPTCHA.....14
Figure 2.5: An Example of Audio-Based CAPTCHA.....15
Figure 3.1: Methodology of the thesis.....20
Figure 3.2: Picture Based CAPTCHA.....24
Figure 3.3: Text Based CAPTCHA.....25
Figure 3.4: Arithmetic operation CAPTCHA.....26
Figure 3.5: No CAPTCHA reCAPTCHA.....26
Figure 3.6: Game based CAPTCHA.....26
Figure 4.1: Gender of participants.....31
Figure 4.2: Age of participants.....31
Figure 4.3: Education level of participants.....32
Figure 4.4: For how many years they have been using the Internet.....32
Figure 4.5: How often they use the Internet.....33
Figure 4.6: Means and Standard Deviations forCAPTCHA types.....41
Figure 4.7: familiarity and attitude for each kind of CAPTCHA.....42
Figure 4.8: The success rate for each kind of CAPTCHA.....43
Figure 4.9: The response time for each kind of CAPTCHA.....44
Figure 4.10: Means of attitude regarding to Age.....45
Figure 4.11: Means Deviations of types of CAPTCHA according to Age.....46
Figure 4.12: The Mean of security preference for each kind of CAPTCHA.....47

LIST OF ABBREVIATIONS

CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
DoS	Denial of Service
HIPs	Human Interaction Proofs
ICT	Information and Communications Technology
IDs	Identities
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
SMS	Short Message Service
SPSS	Statistical Package for the Social Sciences
TCP/IP	Transmission Control Protocol/Internet Protocol
W3C	World Wide Web Consortium
WWW	World Wide Web

CHAPTER 1

INTRODUCTION

1.1. Subject Overview

It is evident that information and communications technology (ICT) has changed the perception of the world in the past fifty years to extend its effects towards business, education and services [1]. The Internet nowadays is the great example for applying the concept of ICT, in which thousands of million users around the world are connected together and exchange information over it. The users have different aims and various knowledge levels. The statistics show that the Internet users have increased between June 2014 and December 2017 by 36.9%, where more than a billion new users have joined the Internet in that period [2]. The Internet witnessed a huge increase in both its users and devices, in their kinds and accounts, and as a result, this generated several challenges of security vulnerabilities.

The users of institutes and companies need to keep their information on servers over the Internet where attacks by hackers can be realized. Thus, many websites are now designed to give privilege levels of access to their users. Moreover, studies show that security measures on the Web are continuously developing to cope with the increasing numbers of attacks and growing networks, as well as the continuous changes in the types of attacks and their complexity [3].

Many Information Technology (IT) and web security programmers and developers have developed several applications to protect data from hackers in order to ensure the operational continuity of the networks and platforms. For protecting sensitive and crucial information on the web, several security measures are taken, especially for client data and financial information, which includes implementing access control measures, imbedding identities into applications by the author, encryption, isolation of sensitive information, and providing several permission steps to reach information [4]. Other than the cyber-attacks that are performed by hackers, cyber criminals have designed bots for the purpose of scraping, spamming and initiating

Denial of Service (DoS)-based attacks, which forms a new type of automated attacks [5].

The web security specialists have developed Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) in order to be able to distinguish the actual human users from bots [6]. CAPTCHA is a kind of methods that is used for determining the users that are permitted or have the authority to access a website or a file on the Internet. This is achieved by designing and implementing the CAPTCHA on the website with a level of complexity corresponding to the degree of importance of information on the website and to the types of users allowed.

Several types of CAPTCHA are used around the Web, including text-based, sound-based and image-based [7]. However, studies show that different people have different preferences towards the types of CAPTCHA depending on factors including age, language and gender [8]. Furthermore, there is a debate in the literature towards the type of CAPTCHA that provides the required security and meets the preferences of the users. Thus, some studies have tested the attitudes of the people towards CAPTCHA types but with limited explorations.

Security in electronic services has been enhanced because of the application of CAPTCHA. Also, it may be used in directing marketing campaigns including those for pornography websites or by those who want to flood their opinions into web boards or public blogs without being traced their identities.

The usability of CAPTCHA is one of the important subjects that are necessary to understand when designing the tool. For instance, there are three main issues that face the usability of text-based CAPTCHA, which is one of the most widely used type of CAPTCHA. The first is distortion issues, where the text in the image can be confusing or not understandable by foreigners to the written language of the text. The second is the content issues emerging from its predictability, string length and randomness, and inappropriate words that could be generated. The third is the presentation issues that can be found due to font type and size, image size, and colors used for the text and the background [9].

In addition to the studies identifying and optimizing CAPTCHA designs, other studies attempted to provide certain rules to enhance the usability of the CAPTCHA and eliminate any issues that could cause confusion for the users and security issues for the developers. A usable CAPTCHA should allow the user to get it right at the first time, perform the task quickly, learn the method of usage for next validations, and have a pleasant experience rather than frustrating. In addition to that, the usability means to reduce errors of usage [10].

Since the CAPTCHA has faced many issues and challenges in usability, many other methods are developed to increase the level of security such as, but not limited to, providing the users with unique identifiers such as national security numbers, performing verification via email or Short Message Service (SMS), and prioritizing the development of CAPTCHA that is based on motion. Furthermore, other administrative methods can be used, including; logging the data of the traffic and its nature, checking server-side data, allowing for a minimum response time, providing login Identities (IDs) as an addition to usernames, and providing limitations on the features of the platform such as limited number of emails to be sent [11].

This research emerges to provide a more reliable data that can indicate the attitudes of people towards the different types of CAPTCHA, as well as providing a scale that can measure the CAPTCHA user perception. In this scope, we first develop a scale to measure user attitude, since there is no an available satisfactory one. Then, we investigate the attitudes of university students towards several types of CAPTCHAs designs that are well known nowadays. For this purpose, we use a set of questions listed in a questionnaire that is distributed among students. The answers of that questions depend on the students' experiences for the web, the type of CAPTCHAs they prefer, and the simplicity degree of the CAPTCHAs that require less time to be solved during their navigation on the Internet. For example, some users have attitudes toward using text-based CAPTCHA while others may prefer image or other kinds. Some others think that CAPTCHA is wasting their time. All these attitudes depend on the psychology of users.

1.2. Study Aim and Research Questions

The main aim of this study is to evaluate the attitude of students towards different types of CAPTCHA through development of a measurement scale. The study investigates the most common types of CAPTCHA that are used on the Web. In this scope, the study analyzes the attitudes of students towards CAPTCHA according to demographic and Internet usage information, including gender, age, education level, for how many years they have been using the Internet, and how often they use the Internet. Based on the aim of the study, the following research questions are developed:

1. Are there any differences between user experiences on various CAPTCHA tests?
2. Are there any differences in familiarity of users for each kind of CAPTCHA?
3. Is the success rate different in the various CAPTCHA tests?
4. Is the response time different in the various CAPTCHA tests?
5. Which type of CAPTCHA is considered as a good technique to provide security in websites?
6. Are there differences onuser attitudesregarding to age?

1.3. Thesis Organization

The thesis divided into five main chapters, where the first chapter provides an overview of the topics covered in the study, in addition to the aim of the research. The second chapter includes the literature review, where ICT, web security solutions and challenges, CAPTCHA usage, and people's perception and attitudes towards CAPTCHA are investigated based on the previous studies. The third chapter provides information about the evaluation scale for CAPTCHA perception and attitude developed considering the literature, in addition to the questionnaire which is used for the assessment. Furthermore, the results are presented in the fourth chapter through descriptive statistics and analysis, as well as a discussion of the results in line with the literature findings. The fifth chapter includes the conclusions of the study along with the recommendations and future research.

CHAPTER 2

LITERATURE REVIEW

2.1. Information and Communication Technology (ICT)

The technological advances in recent years have affected communities over the world. Information and Communication Technology (ICT) is the combination of technological means and tools used to communicate, distribute, supply and manage information. The tools of technology contain Internet, computer, television, radio, hardware, software, telephone, etc [12]. ICT means getting information and other facilities from the novel and advanced scientific discoveries and technologies. Therefore, it eases human activities, saves time and increases productivity to a great extent.

During the past twenty years, the ICT usage has essentially altered the practices and procedures of approximately all forms of life. According to Daniels, the ICT have become, within a very short time, one of the elementary blocks of building of novel society [13]. Various countries currently consider understanding ICT, and mastering the basic skills and concepts of ICT as part of the life [14]. The ICT is now a commonplace concept in all aspects of life, becoming very important as the world is growing rapidly into a digitalized media and information society. ICT has become the connection of communication among communities and countries; a tool used for opening opportunities and creating channels for educational, personal and country development.

The term ‘ICT’ was overviewed at near 1992 in previous century, when e-mail began to become obtainable to the public. ICT offered provision of the Internet services, telecommunications equipment and services, information technology equipment and services, media and broadcasting, centers of libraries and documentation, commercial information, services of network-based information, and other related information and communication activities. Several types of ICT products have significance, such as teleconferencing, email, audio conferencing, television lessons,

radio broadcasts, interactive radio counseling, interactive voice response system, audiocassettes and CD-ROMs, etc. [14].

The widespread adoption of ICT has created several critical threats to information privacy as following:

1. The ICT permits huge amount of private data to share by several users and institutes.
2. Absence of exact privacy information about the action or preferences of specific users are a weakness [15].
3. Widespread adoption of ICT may lead to loss of control of information that is potentially private and shared between business partners.
4. The threat associated to the ownership or private or sensitive data is another problem, for example if you have shared your private data with an organization, the organization may not protect it sufficiently well [16].

Several techniques have proposed to avoid those threats in last two decades, such as access authorization, restricted access, encryption algorithms, and granted privileges. CAPTCHA is also one of the techniques developed for the same purpose.

2.2. Internet Security Challenges

The growing Internet generates a number of opportunities and applications that were not imaginable before. A clear example is the Internet of Things (IoT). IoT is a system of network that contains several applications and wired or wireless smart sensors. Dissimilar attacks and threats could cause serious disasters to an IoT system without the crucial security guard. Thus, the security and administration of the IoT system become quite important [17].

A brute force invasion is proved to be dangerous for the operators at the nodes of Internet. This intrusion takes up a lot of space allocation, time, and resources; however, if we manage to execute certain security measures, then it would make it less susceptible for attackers to use this force to hack into the user's system. Some of the precautionary measures would be [18]:

- Having a complex (e.g., alphanumeric or a mix of special symbols) or lengthy password.
- Restrict the number of attempts to sign into the account. And in the case of failure to log in within the given limits, the account should be provisionally inaccessible. For instance, when one enters the incorrect password multiple times in a Gmail login, there is a CAPTCHA code automatically sent along with a request to enter the text in the image which is generated by the system. This is done to check whether the password is being entered by a program/robot or is being entered by the human, that Gmail is unaware of [19].

Threats can generally be defined as any potentially adverse occurrence or an unwanted event that could injure either the system or the network. Threats are of many different types [20]:

- Alteration: Making changes to the system without authorization.
- Denial of service: A facility or system is unavailable to users due to destruction or damage.
- Errors and omissions: An intentional or unintentional error or omission in the system.
- System malfunction: Typically, the result of hardware or software incompatibility or poor system design.
- Fraud or theft: Theft of the system or access to the system resulting in a scheme to defraud.
- Unauthorized disclosure: The system, data, or configuration disclosed to unauthorized people or processes.
- Regulatory and contractual exposure: Failure to comply with requirements resulting in penalties or damages.

A security threat may be defined as a circumstance or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, and modification of data, denial of service, and/or fraud, waste, and abuse. Besides those threats, Internet users need to contend with a lack of international supervision, rules and standards [21].

2.2.1. Lack of International Supervision

Internet users cannot rely on an internationally recognized set of regulations regarding data protection. There is no central mechanism or “network control center” that supervises the flow of data. Moreover, the increasing use of web technologies can only exacerbate this situation with users downloading software and data from an increasing number of sources located anywhere in the world.

2.2.2. Lack of International Data Protection Standards/Legislation

The lack of a "network control center" means the responsibility for data protection and data security is shared between millions of providers. Every message transmitted could be intercepted at any unsecured site it passes and could be modified, spoofed (falsified), cancelled or delayed. In most cases, users have no control over the route a particular packet takes when it is transmitted to the Internet. Nevertheless, the Internet used for business purposes is increasing exponentially, and many users are using it to transmit personal data.

Despite the increasing popularity of the Internet, an immense amount of work needs to be done at national and, especially, international levels to specify and implement data privacy regulations and laws.

2.2.3. Authentication/Identification Requirements

The use of the Internet services does not allow for adequate anonymity nor adequate authentication. A typical Internet packet contains a header with information about the sender and the recipient (name and Internet Protocol (IP)-address, host name, timestamp, etc). The header contains further information on the routing and the type of packet transmitted. Web and e-mail users leave an electronic trace, which can be used to develop a profile of personal interests and tastes.

Although there is no central accounting of the access to news or World Wide Web (WWW) sites, the information behavior of senders and recipients can be traced and supervised at least by the Internet Service Provider (ISP) to whom the user is

connected. Most ISPs will deny using this information, but the fact remains that they are technically capable of gathering it.

Although profiling users' habits represents a real privacy threat, the major security risk related to the lack of proper identification and authentication features is the vulnerability of systems to hacker attacks. These attacks range from malicious pranks (such as displaying messages on particular dates), to destroying and / or compromising sensitive data. Another common attack is to charge another user's account for Internet services [22].

2.2.4. Confidentiality Requirements

By connecting to the Internet, users are exposing themselves, and their organizations, to the entire population of this very large network. Expectations of confidentiality and privacy should be, but often are not, reduced by that exposure. In other words, many users tend to expect the same data protection and security features enjoyed during the times of private data networks. Having said that, it is vital for network and service providers to make sure that those expectations of confidentiality are met.

The popularity of electronic commerce transactions depends mainly on the confidentiality of sensitive data such as credit card numbers and the integrity of electronic cash mechanisms.

2.2.5. Interruption of Service

Recent attackers to Internet sites have used a technique called "SYN flooding". The attackers use the fact that Transmission Control Protocol/Internet Protocol (TCP/IP) attempt to start data transmissions by using ACK and SYN ACK packets.

The flooding takes place when the attacker's computer does not acknowledge the attacked computer's SYN ACK, and it continues to "flood" the computer with SYN packets. At the moment there are not accepted ways of combating this attack and in several cases complete sub-networks have been disconnected from the Internet in an

attempt to control the problem. This is just an example of interruption or denial of service.

2.2.6. Masquerading

Masquerading takes place when a user pretends to be somebody else. The IP spoofing (using somebody else's IP address) attack has been used to charge another user for commercial services accessed via the Internet, or to cause damage to a remote computer while incriminating an innocent user. Some hackers use a "chain" of spoofed IP addresses to hide their location or to hinder the tracing of their original network address.

2.2.7. Repudiation

Repudiation occurs when a user claims that a particular message has not been sent or that the received message is different from the original. For example, a user may argue that a withdrawal message was never sent to the bank, or that the amount withdrawn was different from the amount claimed by the bank for that transaction.

2.3. CAPTCHA Definition and Usage

Malicious programs attempt to access websites for several purposes. One of the key problems of cyber security is to understand whether the agent attempting to access a website is an actual person or a malicious automated program (“bot”). Web applications need to distinguish human users from an automated tool. Several automated tools can be utilized for malicious purposes, like scraping, spamming, and application-level DoS attacks. For this purpose, there is a technique named CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) used as a common security measure at present against automated attacks [23].

CAPTCHA is defined by several researchers but all definitions agree on the point that it's a method of test ensuring that only persons can answer to its questions, robots or computer programs cannot.

A CAPTCHA can be defined as a program that produces and grades tests that are human solvable, but outside the abilities of present programs of computers [24]. This technology is nowadays often a standard security approach for treating unwanted or malicious Internet bot programs and has created widespread application on many commercial web sites [25].

Another definition is that a CAPTCHA is a program that keeps websites against bots by producing and grading tests that humans can pass but current computer programs cannot. For example, humans can read slanted text as the one shown in Figure 2.1, but current programs cannot [26].

CAPTCHA is also known as human interaction proofs (HIPs). Its design is far from trivial because the challenge is that it should be solved simply by humans, while it should be too hard for computers to solve [27].

Figure 2.1: Concept of CAPTCHA

There are three elementary features that a CAPTCHA should satisfy [28]:

1. It should be easy enough for a user to share and pass the test.
2. It should be simple for tester machine to produce and grade.
3. It should virtually accept all human users and discard software robots.

2.3.1. CAPTCHA Use

The usage of CAPTCHA spreads widely over different sectors from stocks to blogs. In other words, wherever there is human interaction over the web, a CAPTCHA

should be installed. This makes the network safe from bots or web crawlers. The CAPTCHA can be used in several applications as follows:

1. Protecting website registration: CAPTCHAs are utilized to protect several free E-mail services such as Yahoo, Gmail, and Hotmail from Bot programs, that would register thousands of email accounts every minute using automated script.
2. Protecting email addresses from scrapers: This can be done by hiding a user's email address from Web scrapers by asking the user to solve a CAPTCHA before displaying his or her email address [27].
3. Online polls: CAPTCHAs are also utilized to restrain Web crawlers and bots from engaging in online polling by asking the user who wants to vote to solve a CAPTCHA before the vote submission. However, this process cannot prevent users from voting many times.
4. Preventing from dictionary attacks: This is to restrain computer programs from being able to repeat through the entire space of password by asking the user to solve a CAPTCHA test after a number of unsuccessful logins. This mechanism is better than locking an account after a certain number of unsuccessful logins.
5. Search engine bots: CAPTCHAs can be utilized by administrators to stop search engines from indexing to prevent others from downloading or reading these sites because sometimes they contain private information [28].
6. Fake accounts: A bot can disguise himself as a registered user and can create multiple fake accounts; this is one of the reasons for getting spam emails, commenting the blogs by using different names, etc.
7. Denial of service: This is a most common attack which will be found on the web-servers, when a web server is compromised it throws a DOS error. Captcha's can be used on web servers to prevent these attacks.
8. Online reviews: Most of the online products are associated with reviews, "*A user gave 1000 1-star reviews to an Amazonproduct*". Amazon, the famous website was compromised once and lost its users reviews [29].

2.3.2. CAPTCHA Attacks

Understanding different CAPTCHA attacks gives an enhanced understanding on the different types of CAPTCHA [29].

- **Bot Attacks:** This is one of the most common CAPTCHA attacks, different types of web-crawlers or bots are used to break the CAPTCHA. CAPTCHA's are placed at the login page of the web pages and upon solving them, the user will be granted access to enter the webpage. In this attack, bots act themselves as users and try to solve the CAPTCHA (by using preinstalled algorithms) and mask themselves as humans and gain access over the webpage. In order to protect the webpage from the bots, the CAPTCHA should be designed in such a way that the user alone could resolve it and the bot should not.

- **Human Resolvers:** They are considered as the biggest threat for the current CAPTCHA's, one such example is the Death by CAPTCHA. Both the bots and the humans will be working together to resolve CAPTCHA's. This is a paid service, and the CAPTCHA's will be solved by humans. An automated web scraping tool (bot) gathers multiple CAPTCHA's and will send to the human resolvers and those resolvers input the solved CAPTCHA back to the tool, thus the bot gains the access over the webpage.

2.3.3. Types of CAPTCHA

There are several types of CAPTCHAs that are used as a security measurement in websites in order to distinguish human users from Bots. Mostly used CAPTCHAs are as follows:

a. Text-Based CAPTCHA: In text-based CAPTCHA, characters are distorted and connected to prevent recognition by Bots. Some text-based CAPTCHAs are given in Figure 2.2 [26].

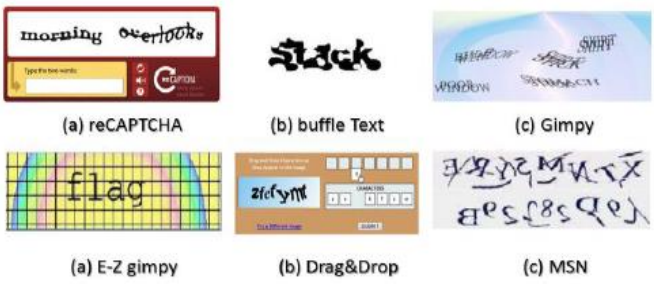


Figure 2.2: Some Examples of Text-Based CAPTCHA

b. Image-based CAPTCHA: In image-based CAPTCHA, the user is provided with a small set of images to name or differentiate or identify anomalies. Here users need to click on images. Bots find difficulty in identifying images. Various implementations of image-based CAPTCHAs are given in Figure 2.3 [27]:

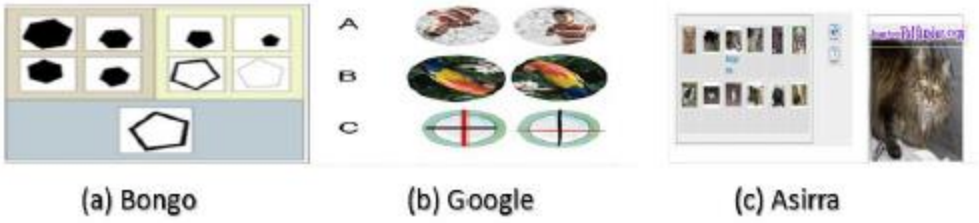


Figure 2.3: Some Examples of Image-Based CAPTCHA

c. Multi Model CAPTCHA: It uses both text and image-based systems together. Here images with multiple text labels are given. User needs to select the right text label [28]. An example is given in Figure 2.4.

Figure 2.4: An Example of Multi-model CAPTCHA

d. **Audio-Based CAPTCHA:** It takes a random sequence drawn from recordings of simple words or numbers, combine them and add some disturbance and racket to it. This soundtrack played when the user clicks a button given on the web page. The CAPTCHA system then asks the user to enter the words and/or numbers in the recording as shown in Figure 2.5.

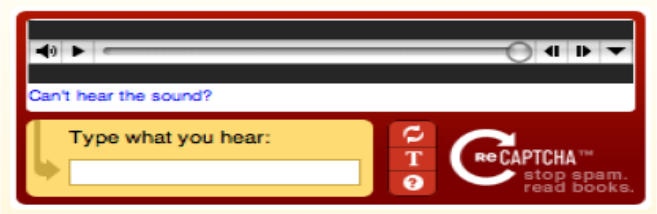


Figure 2.5: An Example of Audio-Based CAPTCHA

e. **Video-Based CAPTCHA**: Here three words (tags) are offered to user which explains a video. If a user's tag belongs to a set of automatically generated position fact tags, then a challenge is passed [27].

2.4. Attitudes towards CAPTCHA

Internet users are highly aware of CAPTCHA. But although users are aware of CAPTCHA, their understanding of it may be somewhat superficial. In examining such a tool there are several scales that must be adopted and adjusted based on previous studies on examining attitudes towards similar concepts.

Researchers have pointed out that one's attitude is a result of his or her perception. That is, a person must perceive an object and subsequently develop an evaluative statement of the object. Such an evaluation is captured in favorable or unfavorable attributes.

The three most required behavior scales are:

(1) There may be additional better methods to perform what CAPTCHA can perform.
(2) The CAPTCHA could offer the services only for those knowing English.
(3) CAPTCHA is effective.

Based on these three items, it seems that the Internet users may agree to the large extent on CAPTCHA's positive attributes (i.e., effectiveness, good support),

although they perceive CAPTCHA as possibly not being the best way to distinguish between man and machine (i.e., better tools than CAPTCHA may exist) [30].

There are several researches concerned with the attitudes of users towards CAPTCHA through navigating on the web. Here, we mention some of researches.

Chatpong and Paradorn investigated awareness and attitudes of Internet users for CAPTCHA and concluded that their understanding does not go very deep. Using exploratory factor analysis, they classified their attitudes towards CAPTCHA in two dimensions: (1) the perceived drawbacks of the CAPTCHA test and (2) the feasibility of CAPTCHA in Thai language. They concluded that online service providers could take certain measures to improve users' attitudes and understanding regarding to CATPCHA [31].

Christos, Nikolaos and Artemios performed a study to examine how the differences among many CAPTCHA tests affect the user experience in two cases: with and without learning disabilities. They prepared a questionnaire including five different tests and they distributed that questionnaire to 212 users, 60 of them with learning disabilities while 152 of them without learning disabilities. They collected response rates automatically for each test. Findings suggested that users with learning disabilities have more difficulties in solving the tests, especially those with distorted texts have more negative attitudes towards the CAPTCHA tests, but the response time has no statistical difference from users without learning disabilities. These insights can help to develop and implement solutions suitable for many users and especially for population with learning disabilities [32].

Jeff and Salahperformed a questionnaire-based survey in order to explore many features that affect end-user perceptions associated to the quality of CAPTCHA. They used a total of 210 participants of age between 19 and 64 years, during May and July 2010. The survey results validated the common belief that CAPTCHAs are still difficult for humans to solve. They also discussed usability issues that should be considered and addressed in the design of CAPTCHAs. Some of these issues are intuitive, but some others have subtle implications for robustness (or security). Also,

they proposed a simple but novel framework for examining usability of CAPTCHA [24].

2.5. Usability of CAPTCHA

CAPTCHA is now almost a standard security technology, and has found widespread application in websites. Usability and robustness are two fundamental issues with CAPTCHA, and they are often interconnected with each other.

The terms accessibility and usability are often used interchangeably in the area of information technology; however, these two terms do not share the same meaning.

The usability is determined by how well a specific user group can complete a task, whereas accessibility is determined by how well a diverse group of users can complete a task [33].

There are some usability issues that should be considered in the design of CAPTCHAs and they are very important, but some others have subtle implications for robustness (or security).

Nielsen's usability measurements are designed to evaluate how usable a product is [34]. These measurements can be used as a design tool or as a testing tool [35]. Using these measurements during design can help designers and developers to better understand the positive and negative impact that their designs produce [36]. Evaluating products using these measurements is a good method for obtaining data regarding a product's usage. It can determine errors in the system, latency issues and give an understanding to the overall user experience [34].

Five factors evaluated during this testing process:

- Learnability is defined by how easy it is for a user to complete elementary tasks during their first encounter with a product.
- Efficiency is defined by how fast a user can complete a task once they have become familiar with the product.
- Memorability relates to how easily a user can re-establish proficiency following a period of time of not using the product.

- The rate of failure factor refers to how many errors happen while an individual is using a product and how easy it is for that person to recover from these errors.
- The last characteristic is satisfaction which relates to the level of user satisfaction experience while using the product.

It is widely accepted that a good CAPTCHA must be both robust and usable. The robustness of a CAPTCHA is its strength in resisting adversarial attacks, and this has attracted considerable attention in the research community [35].

The CAPTCHAs can pose a major accessibility problem to "users who are blind, have low vision, or have a learning disability such as dyslexia". However, CAPTCHA design should be "human friendly" [36].

The nature of CAPTCHAs determines that the following usability criteria are applicable to address efficiency, errors and satisfaction:

- Accuracy: how accurately can a user pass a CAPTCHA challenge? For example, how many times she has to try in order to pass a test?
- Response time: how long does it take for a user to pass the test?
- Perceived difficulty/satisfaction of using a scheme: What is the perceived difficulty to use a CAPTCHA? Are users subjectively satisfied and would they be willing to use such a scheme?

This set of criteria can be key for (quantitatively) evaluating the usability of CAPTCHAs. However, this set offers little specific guidance on how to improve accuracy, response time or perceived difficulty/satisfaction [34].

2.6 Alternatives to CAPTCHA

There are several alternatives to CAPTCHA that can be used in websites. Some of them are:

a. Logic Puzzles

A logic CAPTCHA is a test that asks a human a question that needs simple knowledge to answer [37]. For example, a logic capture CAPTCHA may ask what day in the week comes after Wednesday or what type of animal barks.

b. Semantic CAPTCHA

A semantic CAPTCHA is a CAPTCHA test that needs a human to make sense of a given sentence. Users must use some kind of semantic reasoning so as to pass the test. A semantic CAPTCHA test may contain a user completing a sentence with a missing word, for example "Stopwatches can _____ numbers". One limitation of this kind of test is that the answer may sometimes be subjective. The answer to the above question could be "count", "time", "display" or "show" [38].

c. Single Sign-on

A single sign-on system permits a user to obtain the access to multiple online resources using a single authorization system. This means that an individual register with an identity provider, and this identity provider then provides global or local authentication to other parties or service providers [39].

An example of a single sign-on system is that of the Microsoft Passport system. A user can generate an account with Microsoft by providing their information, a username and a password. Once a user signs into this account they can access several of Microsoft's online resources without the necessity to sign in again. This means that users can access Microsoft's email, messaging services and social networking systems using one log in facility [40].

d. Biometrics

The World Wide Web Consortium (W3C) propose that an alternate to traditional CAPTCHA is to utilize biometric data to recognize if a user is a person or not. They describe that this biometric solution could executed in combination with a single sign-on logon account (W3C). This kind of system would capture the relevant biometric data of a human being and then use this data to generate an exclusive account user for the individual [33].

CHAPTER 3

METHODOLOGY

The objectives of this thesis are to investigate various CAPTCHA types, students' attitudes towards these CAPTCHA types. Development of a scale to measure user attitudes is also one of the objectives of this thesis. The methodology of the thesis is divided into several stages as shown in Figure 3.1:

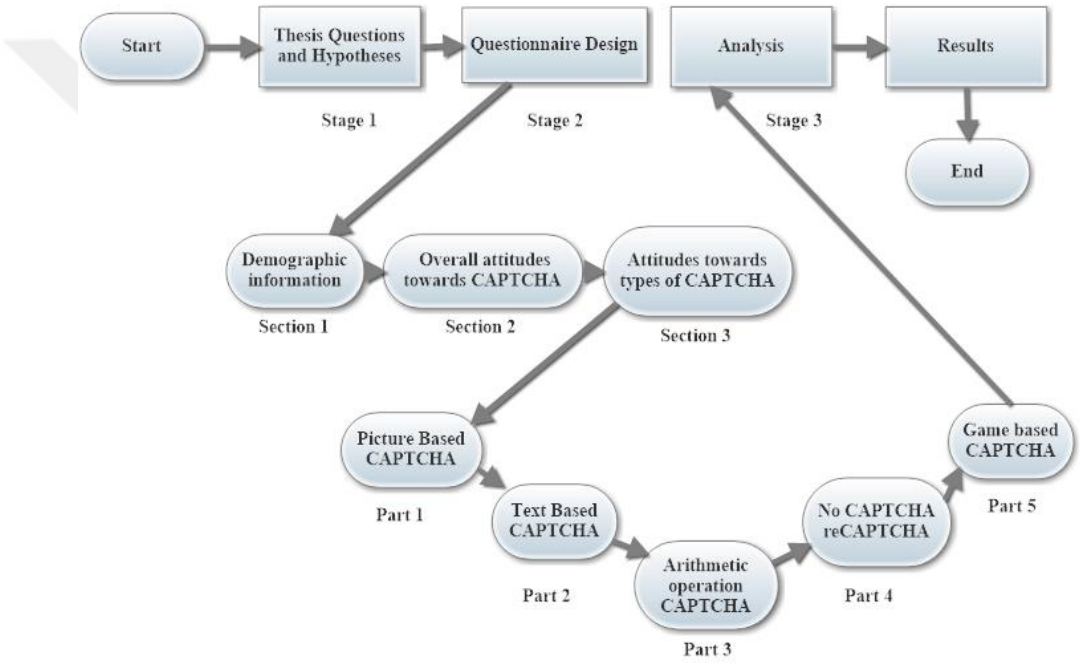


Figure 3.1: Methodology of the thesis

- **Stage 1**: Determination of research questions.
- **Stage 2**: Design of questionnaire, which is based on the research questions. Questionnaire sections will contain different types of questions as following:
    - **Section 1:** contains samples' demographic information through getting the answers of the participants.
    - **Section 2:** contains information of participants overall attitudes towards CAPTCHA [41].

- **Section 3:** contains information of participants' attitudes towards various types of CAPTCHA. This section is based on 5 scales measuring of user attitude towards five types of CAPTCHA [31].

- **Stage 3:** explains the information of used sample of participants together with instrument that is used for analyzing such information.

The following sections of this chapter describe these stages in detail.

3.1. Questionnaire Design

In order to collect data in this research, a questionnaire is created, which includes the actual usage of five different types of CAPTCHA tests. The respondents have to perform the tests and rate their experience using a five-level Likert-type scale (1 – 'Strongly agree', 5 – 'Strongly disagree').

The quality of user experience towards several kinds of CAPTHA's could be examined through this questionnaire, when responding to a test, as well as on the level of test difficulty which reflect the understanding of users.

The questionnaire was composed of:

1- 6 demographic and general information questions.
2- Other 13 questions related to user awareness and understanding of CAPTCHA.
3- And 10 questions for each kind of CAPTCHA; in our study there are 5 kinds of CAPTCHA; thus, there will be 50 questions.

So, each participant had to answer to69 questions in overall.

The types of CAPTCHA that are examined in this research are the following:

1. Picture-based CAPTCHA
2. Text-based CAPTCHA
3. Arithmetic operation-based CAPTCHA
4. No CAPTCHAreCAPTCHA
5. Game-based CAPTCHA

The questionnaire is designed and published as a website in the web in order to make it available for reaching more participants and getting their answers easily. The answers were automatically and anonymously collected into a repository during one month (in March 2018), and then gathered and analyzed using IBM® Statistical Package for the Social Sciences (SPSS)® Statistics.

The design of the questionnaire is divided into several pages according to type of information required. In this scope, the questions are divided into three sections as following:

- **Section 1:** This section gathered the samples' demographic details including screening questions to ensure the subject's eligibility to this current project. It includes six demographic information questions (1-6) with their possible answers. The ages of Bachelor students are in the range of 16-25 years while Master and PhD students have older ages as given below:

Q1: Gender: ○ Male ○ Female

Q2: Age Category: ○ 16 - 20 ○ 21 - 25 ○ 26 - 30 ○ 31 - 35 ○ 36 - 40 ○ above 40

Q3: Education level: ○ Bachelor degree ○ Master degree ○ PhD degree

Q4: What is your department?

Q5: How long have you been using the Internet?

○ Less than 3 years ○ 3 to 5 years ○ 6 to 9 years ○ 10 years and more

Q6: How often do you use the Internet?

○ Every day ○ 3 - 4 days a week ○ 5 - 6 days a week ○ less than once a week

- **Section 2:** This section is devoted to capture samples' awareness and understanding of CAPTCHA. It aims to determine the overall attitudes towards CAPTCHA.

CAPTCHA is defined as a test used in online platforms for security purposes. The test is designed for human visual perception and reasoning in order to allow only humans to pass it but no computers.

The questions (7-19) and their possible choices as answers are the followings:

Q7: Using CAPTCHA is beneficial.

Q8: Using CAPTCHA is important.

Q9: CAPTCHA is enough to verify that the user is human.

Q10: CAPTCHA is credible.

Q11: CAPTCHA is comfortable.

Q12: I do not prefer website that use CAPTCHA.

Q13: CAPTCHA is a waste of time.

Q14: CAPTCHA is frustrating.

Q15: I prefer easy CAPTCHA even if it is less secure.

Q16: I do not trust websites without CAPTCHA.

Q17: I would not enter my personal information to websites without CAPTCHA.

Q18: I would not enter payment information to websites without CAPTCHA.

Q19: Overall, I believe CAPTCHA is needed to an enhance website and information security.

The possible choices as answer for each question are

○ I totally agree ○ I agree ○ neutral ○ disagree ○ I totally disagree

- **Section3:** In this section, 10 questions are devoted to measuring user attitude towards CAPTCHA. The questions were adopted and adjusted for examining attitudes towards CAPTCHA types from some other previous studies [41].

Part A: attitude towards Picture Based CAPTCHA.

Figure 3.2 shows the picture-based CAPTCHA, that user must select required parts of the image then click on the next button for verification.

Figure 3.2: Picture Based CAPTCHA

The following are the questions (20-29) of this part:

Q20: I am familiar with this type of CAPTCHA.

Q21: I believe that this type of CAPTCHA is easy to use.

Q22: I think that this type of CAPTCHA provides enough security.

Q23: This type of CAPTCHA is enjoyable.

Q24: This type of CAPTCHA is friendly and helpful.

Q25: This type of CAPTCHA can be suitable for all users.

Q26: The performed task from this CAPTCHA is easy to understand.

Q27: This type of CAPTCHA does not require a lot of time.

Q28: This type of CAPTCHA does not require a lot of mental effort.

Q29: It is more possible to not make errors using this CAPTCHA.

Possible answer choices for each question are.

○ I totally agree ○ I agree ○ neutral ○ disagree ○ I totally disagree

Part B: Attitudes towards Text Based CAPTCHA.

Figure 3.3 shows the text-based CAPTCHA, in which a user must enter or type the numbers or characters that appear in the image in blank field of an image, and then, click on the Submit button.

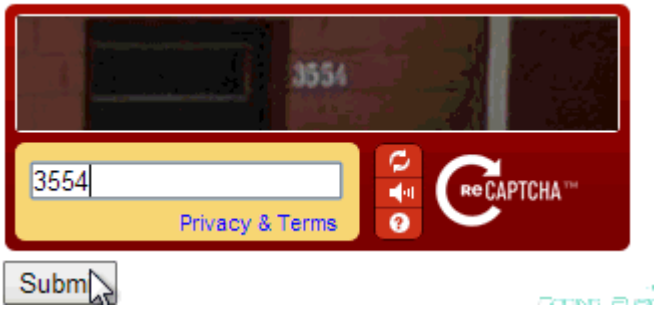


Figure 3.3: Text Based CAPTCHA

The following are the questions of this part (30-39):

Q30: I am familiar with this type of CAPTCHA.
Q31: I believe that this type of CAPTCHA is easy to use.
Q32. I think that this type of CAPTCHA provides enough security.
Q33: This type of CAPTCHA is enjoyable.
Q34: This type of CAPTCHA is friendly and helpful.
Q35: This type of CAPTCHA can be suitable for all users.
Q36: The performed task from this CAPTCHA is easy to understand.
Q37: This type of CAPTCHA does not require a lot of time.
Q38: This type of CAPTCHA does not require a lot of mental effort.
Q39: It is more possible to not make errors using this CAPTCHA.

Possible answer choices for each question are the same as part A.

Part C: Attitudes towards Arithmetic operation CAPTCHA.

Figure 3.4 shows arithmetic type of CAPTCHA in which the user must enter the correct result of the arithmetic operation in the blank field and then, click on the submit button.

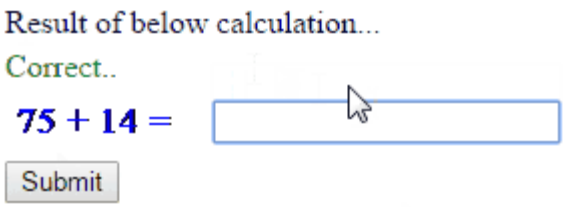


Figure 3.4: Arithmetic operation CAPTCHA

The questions and possible answers of this part (40-49) are the same as in part B.

Part D: Attitudes towards No CAPTCHA reCAPTCHA

Figure 3.5 shows No CAPTCHA reCAPTCHA. This kind needs users to simply click a box to verify that they're a human.

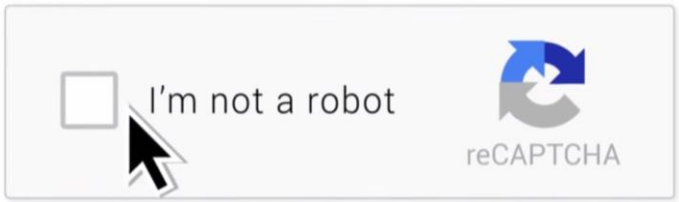


Figure 3.5: No CAPTCHA reCAPTCHA

The questions and possible answers of this part (50-59) are the same as in part B.

Part E: Attitudes towards Game based CAPTCHA

Figure 3.6 shows the game-based CAPTCHA in which the user must play the game in correct manner.

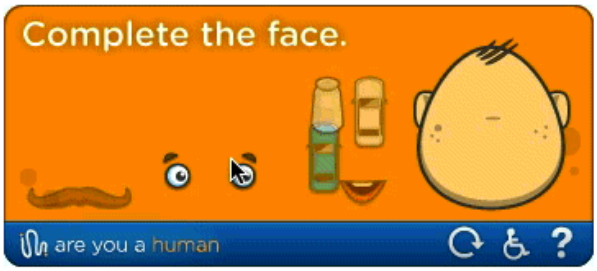


Figure 3.6: Game based CAPTCHA

The questions and possible answers of this part (60-69) are the same as in part B.

3.2. Sample and Analysis

3.2.1. Population and Samples

Given this research's main concern, the samples of population consist of Libyan students which are studying in different Turkish universities and are the Internet users. The number of samples is 145.

Initially, we made an effort to use a probability-based sampling technique. However, we were unable to locate a complete list of Libyan students in Turkey and their contact addresses. As a result, we had to adopt a purposive non-probability sampling through an online contact through the Internet. The offline or papered questionnaire is so difficult to be performed because the students do not respond to this type of questionnaire, we believe that an online questionnaire should be the most feasible means to access to such samples. Once the instrument was ready, we posted an invitation to participate in our project on a number of web boards to which a variety of our target samples had contributed. Although this may pose certain limitation to the findings, it helps access to the distinct group of Libyan students, thereby increasing the study validity. To ensure the reach of only Libyan students, the invitation and the instrument were in Turkey.

3.2.2. Instrument

An online survey approach is used as the instrument to collect data. Our questionnaire consisted of three sections as illustrated previously. At the beginning, the questionnaire drafted and written in paper, reviewed and improved by two experts in information technology. The questionnaire is also pre-tested by seven participants to determine and eliminate possible problems. The finalized version is given in the Appendix.

Once finalizing the content, we converted it into its online version using an open source survey website named https://www.surveymonkey.com/, which makes it possible for every one that want to publish his questionnaire in a website to be answered by users through using the Internet which decrease time and effort.

3.2.3. Data Collection Execution

As explained in the previous sections, we had to adopt the purposive non-probability sampling. We thus approached samples using announcements posted in various means such as mobile phones, social media like Facebook, twitter and so on. The announcement included an invitation to participate in the study, followed by a link to the website containing the questionnaire. The data collection process took about 30 days to achieve 145 usable responses.

3.2.4. Validity and Reliability Issues

To respond to this study's objectives, we strive to ensure the finding's reliability and validity. Such effort includes the followings:

The questionnaire development received our high priority. All items were carefully listed and cleared so that samples would understand them properly. Several rounds of pretests and pilot tests carried to improve the quality. The questionnaire is written on paper and presented to seven students studying at different levels in the university. After pre-testing, the questionnaire was completed.

Once transformed into the online version, the questionnaire is assessed, especially on how a sample would be able to fill in the questionnaire. Such assessment was to ensure (1) robustness of this online version, (2) the smooth flow of answering, and (3) the complete development and conversion of data file for further statistical analysis.

3.2.5. Data Analysis Framework

The framework has two folds. First, we employed descriptive statistics to report (1) the extent to which samples of Libyan students are aware of CAPTCHA and (2) their demographics. Second, we examine broader constructs underlying their attitude towards CAPTCHA, and third we examine broader constructs underlying their attitude towards each type of CAPTCHA.

CHAPTER 4

FINDINGS AND DISCUSSION

After the discussion of the questionnaire design in previous chapter, this chapter outlines descriptive findings and statistical analysis of the obtained results from questionnaire in this study. Demographic data about gender, age category, educational level, department, how long participants have been using the Internet and how often they use the Internet are provided in Section 4.1. Section 4.2 gives the results of statistical analysis for the rest of the answers of the questions in the questionnaire.

4.1. Descriptive Findings

Descriptive statistics are provided by graphs, charts and tables as the result of various descriptive measures such as averages, variation and percentages. In fact, this section mostly deals with descriptive statistics. Descriptive statistics are used to summarize data. Information about different kinds of descriptive statistics are also provided to show how they are calculated.

4.1.1. Demographic Information of Participants

Table 4.1 presents the main features of survey participants

Table 4.1: Demographic Information of participants

Demographics Criteria	**Available choices**	**Participants Total Number = 148**	
		Number	**Percentage (%)**
Q1: Gender	Male	96	64.86 %
	Female	52	35.14 %
Q2: Age	16-20	5	3.38 %
	21-25	16	10.81 %
	26-30	37	25.00 %

	31-35	38	25.68 %
	35-40	30	20.27 %
	Above 40	22	14.86 %
Q3: Education level	Bachelor degree	27	18.24 %
	Master degree	87	58.78 %
	PhD. degree	34	22.97 %
Q4: Study department	Industrial engineering	4	2.7 %
	Information Technology	30	20.3 %
	Computer engineering	17	11.5 %
	Physics	4	2.7 %
	English	15	10.1 %
	Mathematics	5	3.4 %
	Chemical Engineering	14	9.5 %
	Medical technique	9	6.1 %
	Mechanics	12	8.1 %
	Law	18	12.2 %
	Electricity	4	2.7 %
	Nursing	1	0.7 %
	Chemistry	15	10.1 %
Q5: For how many years they have been using the Internet	Less than 3 years	11	7.43 %
	3-5 years	42	28.38 %
	6-9 years	71	47.97 %
	10 years or above	24	16.22 %
Q6: How often they use the Internet	Every day	140	94.60 %
	3-4 days in a week	2	1.35 %
	5-6 days in a week	6	4.05 %
	Less than once in a week	0	0.0 %

The gender of the most respondents was male with 96 participants, approximately 65%, which is approximately twice of females as seen in Figure 4.1.

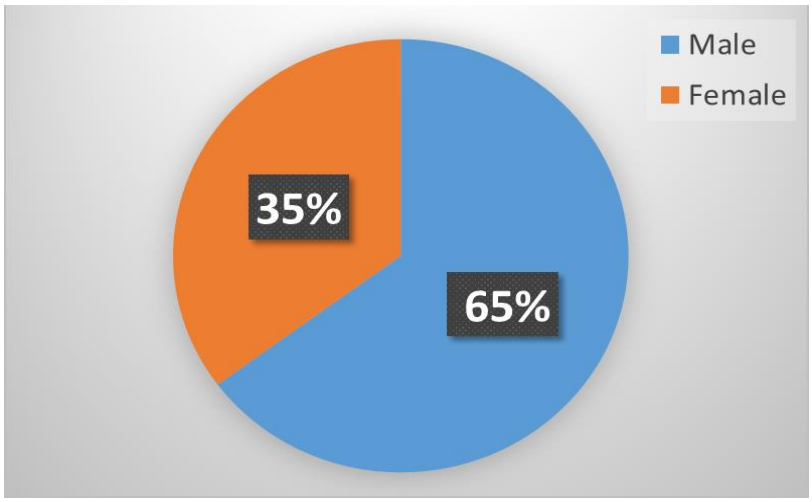


Figure 4.1:Gender of participants

38 of them, approximately 26%, were 31-35 years old which shows the most populated range as seen in Figure 4.2.

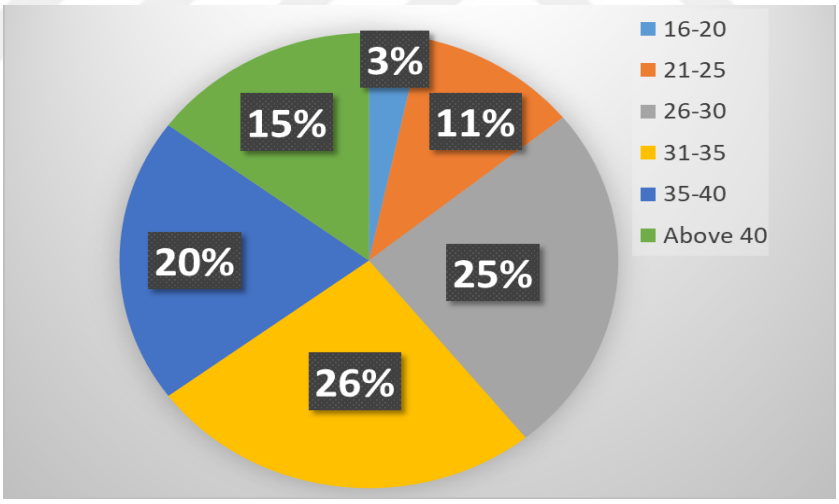


Figure 4.2:Age of participants

Figure 4.3 shows that the largest portion with 87 participants, approximately 59% of them, are now studying to get master degree.

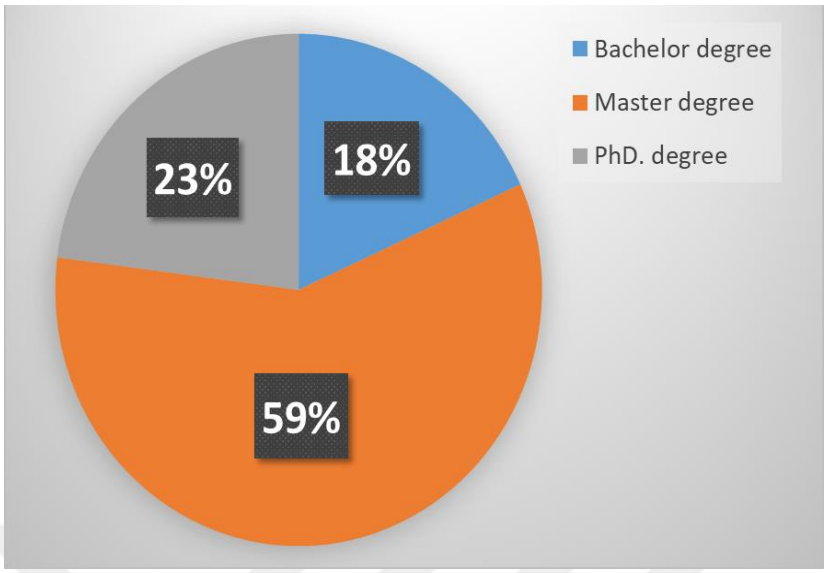


Figure 4.3:Education level of participants

20.3% of participants are students in IT related departments and the rest are students in different departments.

Figure 4.4 illustrates that 71 of participants, approximately 48%, have been using the Internet for 6-9 years.

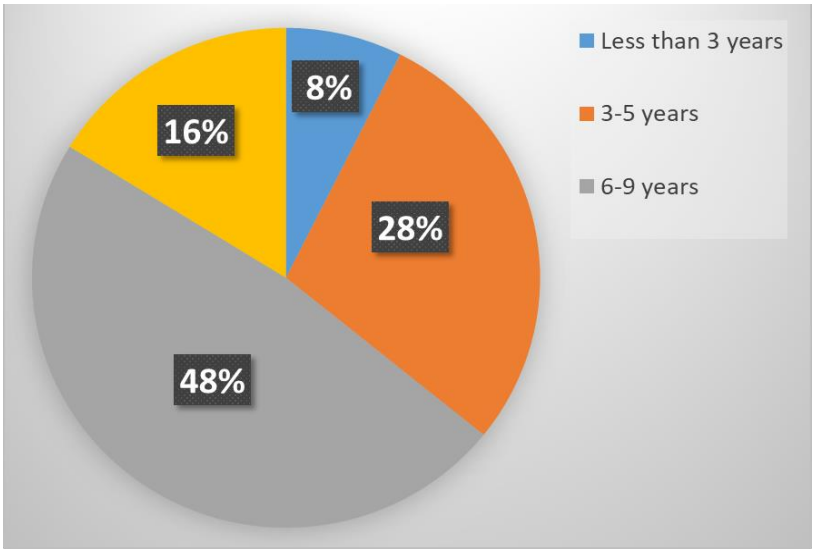


Figure 4.4:For how many years they have been using the Internet

140 of them, approximately 95%, navigate in the Internet every day as illustrated in Figure 4.5.

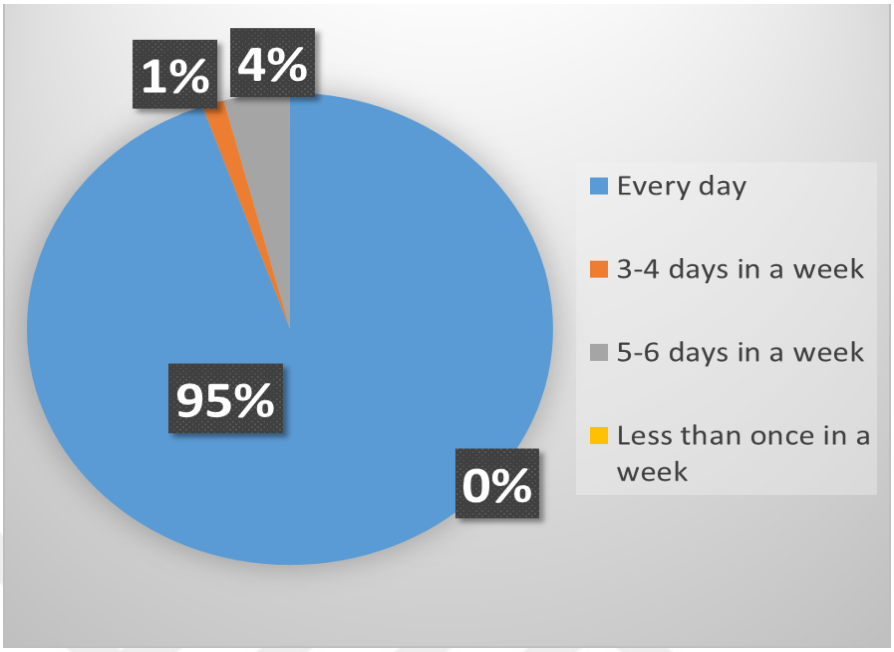


Figure 4.5: How often they use the Internet

4.1.2. Students Understanding and Awareness of CAPTCHA

The questionnaire includes 13 questions to measure the participants' attitudes towards CAPTCHA. They were asked to rate 1 if they totally agree to the criteria or 5 if they totally disagree. Descriptive statistics of these 13 questions are illustrated in Table 4.2. The three most preferred attitude scales are (1) CAPTCHA is credible, (2) Overall, I believe CAPTCHA is needed to enhance website and information security and (3) Using CAPTCHA is important. The question Q7 has the largest score for I totally agree while Q13 has the largest score for I totally disagree.

Depending on these three items, it seems that the participants agree to the large extent on CAPTCHA's positive attributes (i.e., effectiveness, good support for Internet users), while they perceive CAPTCHA as possibly not being the best way to offer security for their necessary information (i.e., better tools than CAPTCHA may exist) and rather to use websites that don't use CAPTCHA.

Table 4.2: Descriptive statistics of these 13 questions

Descriptive criteria. N = 147	**I totally agree**	**I agree**	**neutral**	**Disagree**	**I totally disagree**	**Mean**	**Standard Deviation**
Q7: Using CAPTCHA is beneficial	31	42	55	19	0	2.42	0.965
Q8: Using CAPTCHA is important	18	45	66	18	0	2.57	0.860
Q9: CAPTCHA is enough to verify that the user is human	21	47	59	19	1	2.54	0.923
Q10: CAPTCHA is credible	14	45	70	18	0	2.63	0.821
Q11: CAPTCHA is comfortable	24	38	64	21	0	2.56	0.930
Q12: I do not prefer website that use CAPTCHA	22	39	61	22	3	2.63	0.981
Q13: CAPTCHA is a waste of time	18	34	21	69	5	3.06	1.154
Q14: CAPTCHA is frustrating	18	39	67	20	3	2.67	0.931
Q15: I prefer easy CAPTCHA even if it is less secure	26	37	63	19	2	2.55	0.974
Q16: I do not trust websites without CAPTCHA	24	35	70	18	0	2.56	0.908
Q17: I would not enter my personal information to websites without CAPTCHA	22	36	70	19	0	2.59	0.898
Q18: I would not enter payment information to websites without CAPTCHA	27	40	60	20	0	2.50	0.946
Q19: Overall, I believe CAPTCHA is needed to enhance website and information security.	17	49	63	18	0	2.56	0.853

On the other hand, the participants totally disagree on two attitudinal items: 1. CAPTCHA is a waste of time and 2. I do not prefer website that use CAPTCHA.

The neutral choices may indicate not having any attitudes towards CAPTCHA. As such, participants of this questionnaire are not familiar with CAPTCHA that they see it is not useful. These results is based on Libyan students' attitudes towards CAPTCHA and it could be changed if students of other countries participate in that questionnaire such as Turkish students for example.

4.2. Statistical Analysis

After explaining the descriptive statistics, we will explain the statistical analysis of answers given to questionnaire questions regarding five types of CAPTCHA.

4.2.1. Attitudes towards picture-based CAPTCHA

Table 4.3 illustrates the participants' attitudes for picture-based CAPTCHA. 32 of participants selected 'I totally agree' on Q20 (I am familiar with this type of CAPTCHA) while 38 of them selected 'I totally disagree' on Q29 (It is more possible to not make errors using this CAPTCHA). The smallest variance among participants was in Q26 (The performed task from this CAPTCHA is easy to understand) with a standard deviation of 0.844 while the largest variance among them was in Q29 (It is more possible to not make errors using this CAPTCHA) with a standard deviation of 1.052. The overall mean value is 2.819 while overall standard deviation is 0.927.

Table 4.3: Attitudes towards picture-based CAPTCHA

Attitude item N= 146	**I totally agree**	**I agree**	**neutral**	**Disagree**	**I totally disagree**	**Mean**	**Standard Deviation**
Q20: I am familiar with this type of CAPTCHA	32	39	57	18	0	2.42	0.967
Q21: I believe that this type of CAPTCHA is easy to use	20	44	63	19	0	2.55	0.887
Q22: I think that this type of CAPTCHA provides enough security	25	41	61	19	0	2.51	0.927
Q23: This type of CAPTCHA is enjoyable	18	45	63	20	0	2.58	0.877
Q24: This type of CAPTCHA is friendly and helpful	29	40	58	19	0	2.46	0.955
Q25: This type of CAPTCHA can be suitable for all users	18	48	59	21	0	2.57	0.886
Q26: The performed task from this CAPTCHA is easy to understand	15	49	63	19	0	2.59	0.844
Q27: This type of CAPTCHA does not require much time	5	74	17	33	17	3.55	0.962
Q28: This type of CAPTCHA does not require much mental effort	1	66	24	39	16	3.49	0.919
Q29: It is more possible not to make errors using this CAPTCHA	2	15	18	73	38	3.47	1.052
	Mean					2.819	
	Stdev					0.927	

4.2.2. Attitudes towards text-based CAPTCHA

The participants' attitudes for text-based CAPTCHA are illustrated in Table 4.4. 38 of participants selected 'I totally agree' for Q30 (I am familiar with this type of CAPTCHA) while 45 of them selected 'I totally disagree' for Q39 (It is more possible not to make errors using this CAPTCHA). The smallest variance among participants was in Q33 (This type of CAPTCHA is enjoyable) with a standard deviation of 0.869 while the largest variance among them was in Q39 (it is more possible not to make errors using this CAPTCHA) with a standard deviation of 1.031. The overall mean value is 2.863 while the overall standard deviation is 0.935.

Table 4.4: Attitudes towards text-based CAPTCHA

Attitude item N= 146	**I totally agree**	**I agree**	**neutral**	**Disagree**	**I totally disagree**	**Mean**	**Standard Deviation**
Q30: I am familiar with this type of CAPTCHA	38	38	49	18	0	2.34	1.000
Q31: I believe that this type of CAPTCHA is easy to use	29	38	57	19	0	2.48	0.963
Q32: I think that this type of CAPTCHA provides enough security	20	43	62	18	0	2.56	0.886
Q33: This type of CAPTCHA is enjoyable	17	47	60	19	0	2.58	0.869
Q34: This type of CAPTCHA is friendly and helpful	26	40	59	18	0	2.50	0.934
Q35: This type of CAPTCHA can be suitable for all users	19	46	56	22	0	2.59	0.915
Q36: The performed task from this CAPTCHA is easy to understand	19	45	59	20	0	2.58	0.900
Q37: This type of CAPTCHA does not require much time	3	72	17	29	22	3.66	0.943
Q38: This type of CAPTCHA does not require much mental effort	0	63	19	36	25	3.67	0.918
Q39: It is more possible not to make errors using this CAPTCHA	0	15	13	70	45	3.67	1.031
	Mean					2.863	
	Stdev					0.935	

4.2.3. Attitudes towards arithmetic-based CAPTCHA

The participants attitudes toward arithmetic-based CAPTCHA are illustrated in Table 4.5. 29 of participants selected 'I totally agree' for Q40 (I am familiar with this type of CAPTCHA) while 38 of them selected 'I totally disagree' for Q49 (It is more possible not to make errors using this CAPTCHA). The smallest variance among participants was in Q43 (This type of CAPTCHA is enjoyable) with a standard deviation of 0.878 while the largest variance among them was in Q49 (It is more possible to not make errors using this CAPTCHA) with a standard deviation of 1.059. The overall mean value is 2.838 while the overall standard deviation is 0.945.

Table 4.5: Attitudes towards arithmetic-based CAPTCHA

Attitude item N= 146	**I totally agree**	**I agree**	**neutral**	**Disagree**	**I totally disagree**	**Mean**	**Standard Deviation**
Q40: I am familiar with this type of CAPTCHA	29	45	48	20	1	2.45	0.983
Q41: I believe that this type of CAPTCHA is easy to use	20	53	50	20	0	2.51	0.904
Q42: I think that this type of CAPTCHA provides enough security	18	51	54	20	0	2.55	0.887
Q43: This type of CAPTCHA is enjoyable	17	49	57	20	0	2.58	0.878
Q44: This type of CAPTCHA is friendly and helpful	25	39	58	21	0	2.54	0.948
Q45: This type of CAPTCHA can be suitable for all users	26	37	57	21	2	2.58	1.002
Q46: The performed task from this CAPTCHA is easy to understand	21	45	58	19	0	2.55	0.910
Q47: This type of CAPTCHA does not require much time	4	69	20	29	21	3.58	0.988
Q48: This type of CAPTCHA does not require much mental effort	1	61	18	45	18	3.55	0.895
Q49: It is more possible not to make errors using this CAPTCHA	0	14	22	69	38	3.51	1.059
	Mean					2.838	
	Stdev					0.945	

4.2.4. Attitudes towards No CAPTCHA reCAPTCHA

The participants' attitudes toward No CAPTCHA reCAPTCHA are illustrated in Table 4.6. 34 of participants selected 'I totally agree' for Q54 (This type of CAPTCHA is friendly and helpful) while 38 of them selected Q59 (It is more possible to not make errors) using this CAPTCHA with 'I totally disagree'. The smallest variance among participants is in Q55 (This type of CAPTCHA can be suitable for all users) with a standard deviation of 0.904 while the largest variance among them is in Q59 (It is more possible not to make errors using this CAPTCHA) with a standard deviation of 1.151. The overall mean value is 2.748 while the overall standard deviation is 0.890.

Table 4.6: Attitudes towards No CAPTCHA reCAPTCHA

Attitude item N= 146	**I totally agree**	**I agree**	**neutral**	**Disagree**	**I totally disagree**	**Mean**	**Standard Deviation**
Q50: I am familiar with this type of CAPTCHA	33	40	52	18	0	2.37	0.983
Q51: I believe that this type of CAPTCHA is easy to use	76	40	21	4	0	2.53	0.926
Q52: I think that this type of CAPTCHA provides enough security	30	41	54	18	0	2.44	0.961
Q53: This type of CAPTCHA is enjoyable	24	46	54	19	0	2.49	0.927
Q54: This type of CAPTCHA is friendly and helpful	34	36	55	18	0	2.42	0.988
Q55: This type of CAPTCHA can be suitable for all users	21	51	53	18	0	2.50	0.904
Q56: The performed task from this CAPTCHA is easy to understand	26	45	54	18	0	2.47	0.941
Q57: This type of CAPTCHA does not require much time	10	65	13	41	14	3.43	1.016
Q58: This type of CAPTCHA does not require much mental effort	8	57	20	40	18	3.39	1.091
Q59: It is more possible to not make errors using this CAPTCHA	7	12	16	70	38	3.44	1.151
	Mean					2.748	
	Stdev					0.890	

4.2.5. Attitudes towards game-based CAPTCHA

The participants' attitudes toward No CAPTCHA reCAPTCHA are illustrated in Table 4.7. 31 of participants selected 'I totally agree' for Q60 (I am familiar with this type of CAPTCHA) while 41 of them selected Q69 (It is more possible not to make errors using this CAPTCHA). The smallest variance among participants was in Q62 (I think that this type of CAPTCHA provides enough security) with a standard deviation of 0.858 while the largest variance among them was in Q69 (It is more possible not to make errors using this CAPTCHA) with a standard deviation of 1.063. The overall mean value is 2.909 while the overall standard deviation is 0.941.

Table 4.7: Attitudes towards game-based CAPTCHA

Attitude item N= 146	**I totally agree**	**I agree**	**neutral**	**Disagree**	**I totally disagree**	**Mean**	**Standard Deviation**
Q60: I am familiar with this type of CAPTCHA	31	32	55	23	2	2.54	1.038
Q61: I believe that this type of CAPTCHA is easy to use	22	40	57	23	1	2.60	0.958
Q62: I think that this type of CAPTCHA provides enough security	14	51	57	21	0	2.61	0.858
Q63: This type of CAPTCHA is enjoyable	12	53	56	22	0	2.63	0.847
Q64: This type of CAPTCHA is friendly and helpful	23	42	58	20	0	2.54	0.926
Q65: This type of CAPTCHA can be suitable for all users	16	42	59	25	1	2.69	0.922
Q66: The performed task from this CAPTCHA is easy to understand	12	47	60	24	0	2.69	0.860
Q67: This type of CAPTCHA does not require much time	5	66	18	31	23	3.58	1.002
Q68: This type of CAPTCHA does not require much mental effort	0	61	22	35	25	3.64	0.946
Q69: It is more possible not to make errors using this CAPTCHA	0	15	20	67	41	3.57	1.063
	Mean					2.909	
	Stdev					0.941	

4.3. Discussion

Mean is the most commonly used measure of central tendency. It is calculated as the central value of a set of numbers. In a questionnaire, that contains multiple-choice questions, it is computed by adding all the values after multiplying by their weight in the data set and by dividing by the number of observations in it.

The standard deviation is a summary measure of the differences of each observation from the mean. If its value is high, this means that the observations dispersed far from mean value and if its value is low, this means that the values of observations are close or near of mean value.

Table 4.8 summarizes the means and standard Deviations for participants' attitudes towards each type of CAPTCHA.

Table 4.8:Means and standard deviations of attitudes towards different types of CAPTCHA

Kind of CAPTCHA	Mean	Standard Deviation
Picture-based	2.819	0.927
Text-based	2.863	0.935
Arithmetic-based	2.838	0.945
No CAPTCHA reCAPTCHA	2.748	0.890
Game-based	2.909	0.941

From this table, we observe that for all types of CAPTCHA the mean values are between 2 and 3 which indicate that the values are close to the center. The typical choices of participants are 'I agree' which represents 2nd choice and 'neutral' which represents 3rd choice.

If the value of mean is near 1, this indicates that most of participants selected 1st choice which is 'I totally agree'. Conversely, if the value of mean is near 5, this indicates that most of participants selected 5th choice which is 'I totally disagree'.

The No CAPTCHA reCAPTCHA was the type that the participants are converge on it, it has the smallest variance since the standard deviation is 0.890. On the other hand, the arithmetic-based is the type that has the largest variance with a standard deviation of 0.945. A large standard deviation value means that a large amount of variation in the group that is being studied. The standard deviation is smaller when the individuals within the group have values very near to mean value.

Figure 4.6 represents a chart for means and standard deviations of five types of CAPTCHA. The obtained results reflect that the students are familiar with all of these types of CAPTCHA since they may deal with them every day through navigating in the web for searching books or scientific articles or research papers. In this calculation, we include all students with three different educational levels and the two gender as one group.

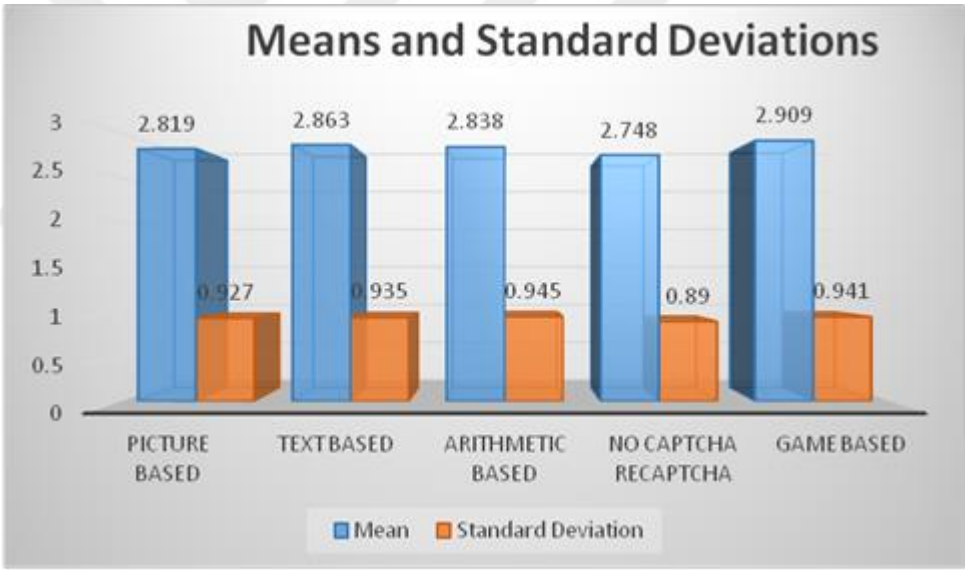


Figure 4.6: Means and Standard Deviations forCAPTCHA Types

With respect to thesis questions:

TQ1: Are there any differences between user experiences on various CAPTCHA tests?

The Figure 5.1 represents a chart for means and standard deviations of five types of CAPTCHA. Differences between user experiences on various CAPTCHA tests are very small. No CAPTCHA reCAPTCHA is mostly preferred one.

TQ2: Are there any differences in familiarity of users for each kind of CAPTCHA?

For measuring the familiarity for each kind of CAPTCHA I have used the question: **I am familiar with this type of CAPTCHA**.

Table 4.9: Familiarity for each kind of CAPTCHA

Attitude item	I totally agree	I agree	neutral	Disagree	I totally disagree	Mean	Standard Deviation
Q20: I am familiar with picture-based type of CAPTCHA	32	39	57	18	0	2.42	0.967
Q30: I am familiar with text-based type of CAPTCHA	38	38	49	18	0	2.34	1.000
Q40: I am familiar with arithmetic-based type of CAPTCHA	29	45	48	20	1	2.45	0.983
Q50: I am familiar with No CAPTCHA reCAPTCHA type of CAPTCHA	33	40	52	18	0	2.37	0.983
Q60: I am familiar with game-based type of CAPTCHA	31	32	55	23	2	2.54	1.038

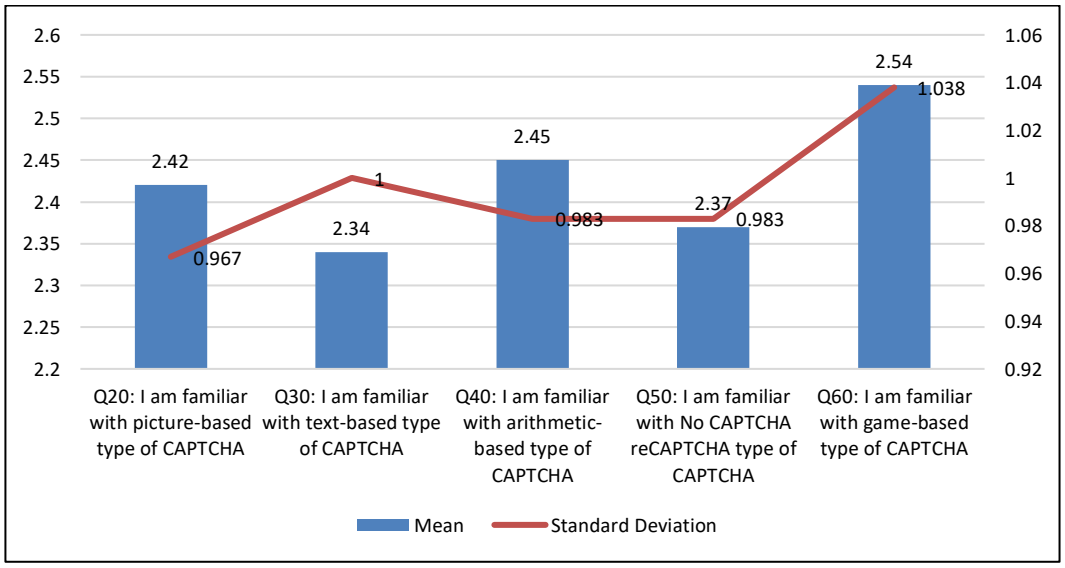


Figure 4.7: familiarity for each kind of CAPTCHA

Participants are more familiar with text-based CAPTCHA followed by No CAPTCHA reCAPTCHA.

TQ3: Is the success rate different in the various CAPTCHA tests?

For success rate I have used this question: **It is more possible to not make errors using this CAPTCHA.**

Table 4.10: The success rate for each kind of CAPTCHA

Attitude item	I totally agree	I agree	neutral	Disagree	I totally disagree	Mean	Standard Deviation
Q29: It is more possible not to make errors using picture-based CAPTCHA	2	15	18	73	38	3.47	1.052
Q39: It is more possible not to make errors using text-based CAPTCHA	0	15	13	70	45	3.67	1.031
Q49: It is more possible not to make errors using arithmetic-based CAPTCHA	0	14	22	69	38	3.51	1.059
Q59: It is more possible to not make errors using No CAPTCHA reCAPTCHA CAPTCHA	7	12	16	70	38	3.44	1.151
Q69: It is more possible not to make errors using game-based CAPTCHA	0	15	20	67	41	3.57	1.063

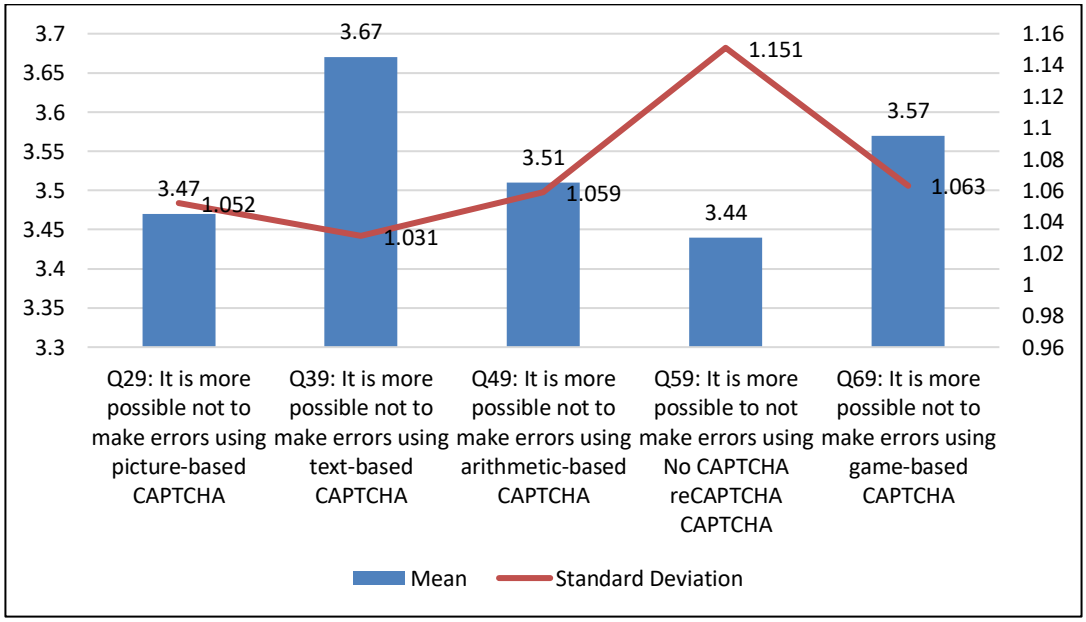


Figure 4.8: The success rate for each kind of CAPTCHA

Participants consider that No CAPTCHA reCAPTCHA is the type having less chance of errors.

TQ4: Is the response time different in the various CAPTCHA tests?

For measuring the response time for each kind of CAPTCHA I have used the question:**This type of CAPTCHA does not require much time.**

Table 4.11: The response time for each kind of CAPTCHA

Attitude item	I totally agree	I agree	neutral	Disagree	I totally disagree	Mean	Standard Deviation
Q27: picture-based type of CAPTCHA does not require much time	5	74	17	33	17	3.55	0.962
Q37: text-based type of CAPTCHA does not require much time	3	72	17	29	22	3.66	0.943
Q47: arithmetic-based type of CAPTCHA does not require much time	4	69	20	29	21	3.58	0.988
Q57: No CAPTCHA reCAPTCHA type of CAPTCHA does not require much time	10	65	13	41	14	3.43	1.016
Q67: game-based type of CAPTCHA does not require much time	5	66	18	31	23	3.58	1.002

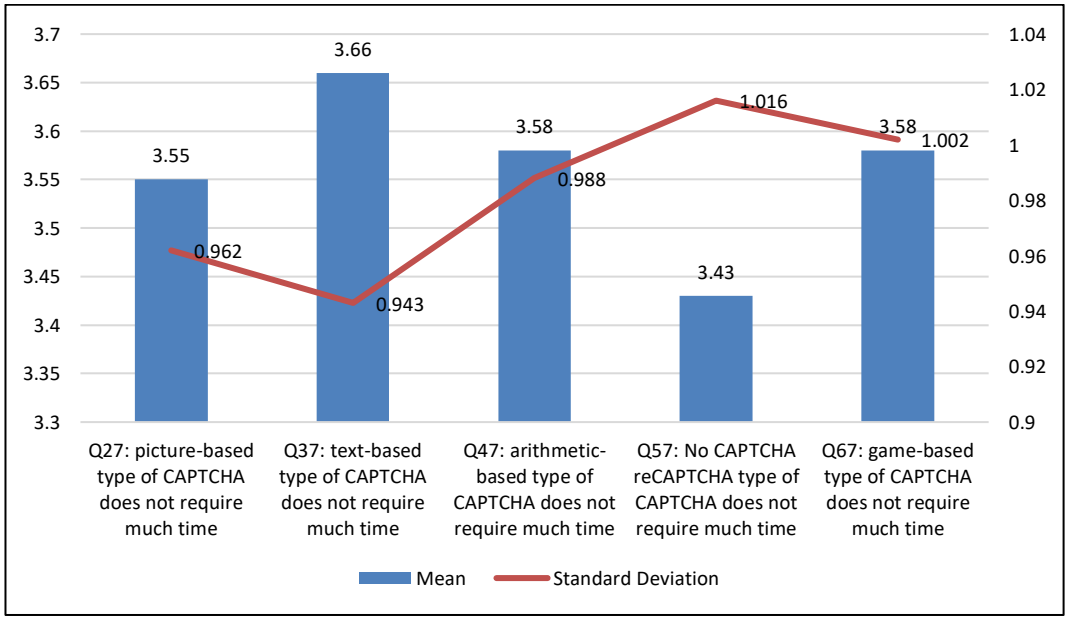


Figure 4.9: The response time for each kind of CAPTCHA

The smallest mean is 3.43 in No CAPTCHA reCAPTCHA kind. It means that participants consider that No CAPTCHA reCAPTCHA kind does not require much time.

TQ5: Are there any differences about the students' attitude for easiness of the various CAPTCHA tests, regarding to their ages?

Table 4.12 illustrates the attitude with regard to age for each kind of CAPTCHA, which represent the answers of participants for the question: **I believe that this type of CAPTCHA is easy to use**.

Table 4.12: Attitude regarding to age

Kind of CAPTCHA	16-20	21-25	26-30	31-35	35-40	above 40	Mean
Picture-based	2	3	2.64	2.36	2.63	2.33	2.49
Text-based	1,66	2,86	2,68	2,32	2,46	2,09	2.34
Arithmetic-based	2	2,86	2,71	2,48	2,76	2,38	2.53
No CAPTCHA reCAPTCHA	1,66	1,66	1,85	1,64	1,66	1,38	1.64
Game-based	2	2,73	2,65	2,59	2,66	2,28	2.48
Mean	1.86	2.62	2.5	2.27	2.43	2.09	

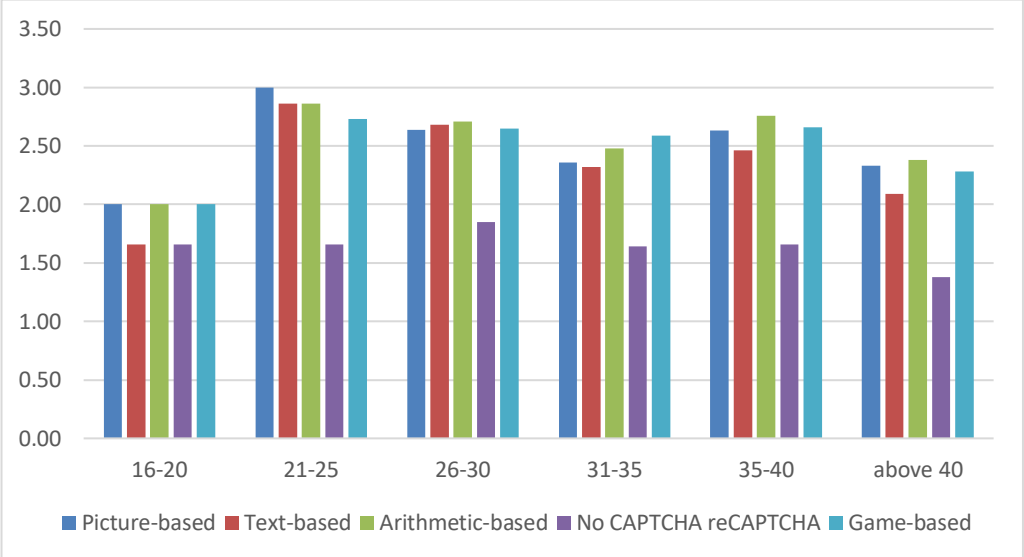


Figure 4.10: Means of attitudesregarding to age

There is no relation between easiness of the various CAPTCHA tests and age. For example, No CAPTCHA reCAPTCHA is considered as the easiest one by all groups. Therefore, age does not affect user attitudes towards CAPTCHA types.

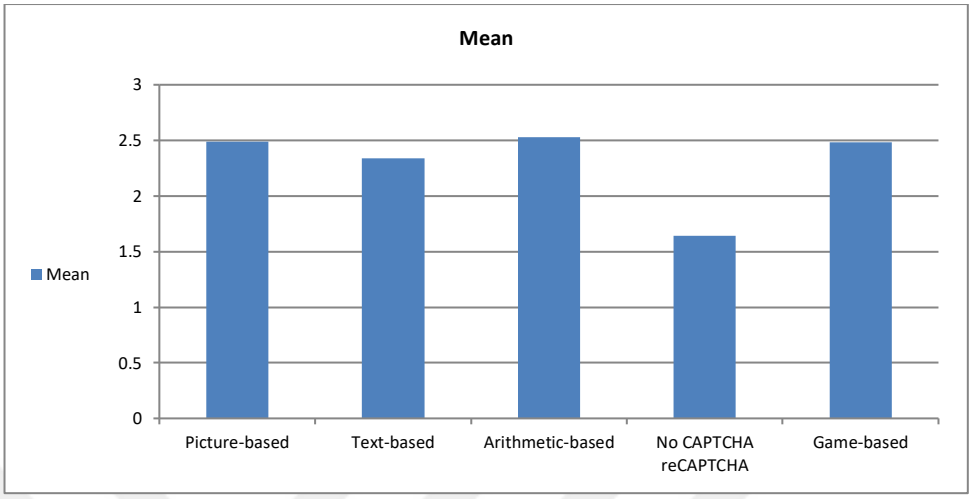


Figure 4.11: Means Deviations of types of CAPTCHA according to Age

TQ6: Which CAPTCHA type is considered as a good technique to provide security in websites?

For measuring the security offered through each kind of CAPTCHA I have used the question: **I think that this type of CAPTCHA provides enough security.**

Attitude item	I totally agree	I agree	neutral	Disagree	I totally disagree	Mean	Standard Deviation
Q22: picture-based type of CAPTCHA provides enough security	25	41	61	19	0	2.51	0.927
Q32: text-based type of CAPTCHA provides enough security	20	43	62	18	0	2.56	0.886
Q42: arithmetic-based type of CAPTCHA provides enough security	18	51	54	20	0	2.55	0.887
Q52: No CAPTCHA reCAPTCHA type of CAPTCHA provides enough security	30	41	54	18	0	2.44	0.961
Q62: game-based type of CAPTCHA provides enough security	14	51	57	21	0	2.61	0.858

Table 4.13: The security preference for each kind of CAPTCHA

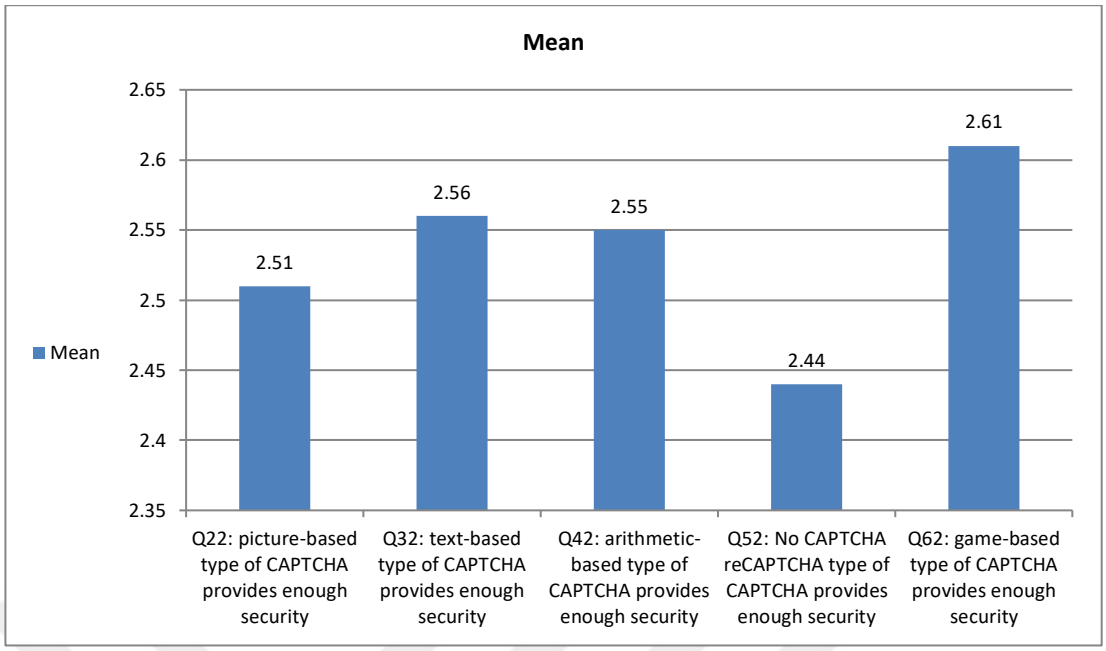


Figure 4.12: The Mean of security preference for each kind of CAPTCHA

Participants agreed that No CAPTCHA reCAPTCHA kind provides more security than the other types.

CHAPTER 5

CONCLUSION AND RECOMMENDITION

5.1. Conclusion

After analyzing the obtained results, the derived conclusions are as follows:

- The participants are more familiar with the text-based CAPTCHA than the others.
- The participants consider that No CAPTCHA reCAPTCHA kind require less time compared to other types.
- In terms of error, the No CAPTCHA reCAPTCHA type is considered the most error free type.
- There is no relation between the age of users and their easiness consideration for CAPTCHA types.
- The participants consider that No CAPTCHA reCAPTCHA provides more security than the other types.
- The No CAPTCHA reCAPTCHA type is the most preferred type.

5.2. Recommendation

As future works, the study can be extended with more participants from different countries and from different fields such as schools, universities, factories, etc. In addition, other types of CAPTCHA can be added to the study. As another study, it is possible to make comparisons among different groups with respect to their attitudes towards CAPTCHA types.

REFERENCES

[1] A. Berisha-Shaqiri, "Impact of informationtechnology and internet in businesses," *Academic Journal of Business, Administration, Law and Social Sciences,* vol. 1, no. 1, pp. 73-79, 2015.

[2] Internet World Stats, "Internet Users in the World by Region - December 31, 2017," 2018. [Online]. Available: https://www.internetworldstats.com/stats.htm.

[3] M. Abomhara and G. M. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security,* vol. 4, pp. 65-88, 2015.

[4] S. Hayikader, F. N. Abu Hadi and J. Ibrahim, "Issues and Security Measures of Mobile Banking Apps," *International Journal of Scientific and Research Publications,* vol. 6, no. 1, pp. 36-41, 2016.

[5] T. Ahmed, K. A. Tushar, S. I. Nova and M. M. Rahman, "Simple, Robust & User Friendly CAPTCHA 'InstaCap' for Web Security," *International Journal of Hybrid Information Technology,* vol. 9, no. 1, pp. 163-183, 2016.

[6] S. Yalamanchili and K. Rao, "A Framework for DevaNagari Script-Based CAPTCHA," *International Journal of Advanced Information Technology,* vol. 1, no. 4, pp. 47-57, 2011.

[7] A. Narula and S. Bhasin, "Survey of Human Interactive Proof and CAPTCHA Techniques and Attacks," *International Journal of Engineering Development and Research,* vol. 4, no. 3, pp. 53-57, 2016.

[8] C. Tangmanee and P. Sujarit-apirak, "An Exploration into Thai Internet Users' Attitudes Towards CAPTCHA," in *The 9th International Conference on Electronic Business*, Macau, 2009.

[9] J. Yan and A. S. El Ahmad, "Usability of CAPTCHAs Or usability issues in CAPTCHA design," in *Proceedings of the 4th symposium on Usable privacy and security*, Pittsburgh, Pennsylvania, USA, 2008.

[10] S. A. Alsuhibany, "A Benchmark for Designing Usable and Secure Text-Based CAPTCHAs," *International Journal of Network Security & Its Applications,* vol. 8, no. 4, pp. 41-54, 2016.

[11] M. Moradi and M. R. Keyvanpour, "CAPTCHA and its Alternatives: A Review," *Security and Communication Networks,* vol. 8, pp. 2135-2156, 2015.

[12] B. Oluwatobi, "The Role of Information and Communication Technology in Education: Case of Eastern Mediterranean University," Gazimağusa, North Cyprus, 2014.

[13] J. Daniels, "“Forward” in Information and Communication Technology in Education – A Curriculum for Schools and Programme for Teacher Development," UNESCO, Paris, 2002.

[14] R. M. Rahman, "An Empirical study of teachers’ and students’ experiences with inclusion and ICT support to blind students," University of Oslo, Oslo, 2017.

[15] T. J. Shaw, Information Security and Privacy, Chicago: Adventure Works Press, 2012.

[16] P. M. Schwartz, Information Privacy, New York: Wolters Kluwer, 2011.

[17] C. Long, "Security Management for The Internet of Things," University of Windsor, Windsor, Canada, 2017.

[18] B. Tripathy and J. Anuradha, INTERNET OF THINGS (IoT) Technologies, Applications, Challenges, and Solutions, CRC Press, Taylor & Francis Group,, 2018.

[19] Y. Huang and G. Li, " Descriptive Models for Internet of Things," in *Proc. of*

Intelligent Control and Information Processing International Conference (ICICIP-2010), 2010.

[20] S. William and B. Lawrie, Computer Security Principles and Practice, 4th ed., Pearson Education Limited, 2018.

[21] J. Lech, Internet and Intranet Security Management: Risks and Solutions, University of Auckland\New Zealand: Idea Group Publishing, 2000.

[22] J. Muysken, "WebTrust and Electronic Commerce," *Charter,* pp. 54-55, 1998.

[23] G. Ruti and N. Idan, "CAPTCHA: Impact on User Experience of Users with Learning Disabilities," *Interdisciplinary Journal of e-Skills and Lifelong Learning,* vol. 12, 2016.

[24] Y. Jeff and E. A. Salah, "Usability of CAPTCHAs or usability issues in CAPTCHA design," in *4th Symposium on Usable Privacy and Security*, SOUPS , 2008.

[25] S. A. Alsuhibany, "A Benchmark for Designing Usable and Secure Text-Based CAPTCHAs," *International Journal of Network Security & Its Applications,* vol. 8, no. 4, pp. 41-54, 2016.

[26] H. W. K. Abdullah, "A SURVEY OF CURRENT RESEARCH ON CAPTCHA," *International Journal of Computer Science & Engineering Survey (IJCSES),* vol. 7, no. 3, 2016.

[27] C. Yashwanth, "AN ORIENTATION BASED IMAGE CAPTCHA," 2009.

[28] A. Tanvir, T. K. Ahmed, N. S. Islam and R. Mahbubur, "Simple, Robust & User Friendly CAPTCHA 'InstaCap' for Web Security," *International Journal of Hybrid Information Technology,* vol. 9, no. 1, 2016.

[29] P. Uday, "I AM NOT A ROBOT: - AN OVERVIEW ON GOOGLE'S CAPTCHA," 2016.

[30] S. Paradorn and T. Chatpong, "AN EXPLORATION INTO THAI INTERNET USERS' ATTITUDE TOWARDS CAPTCHA," in *The 9th International Conference on Electronic Business*, Macau, 2009.

[31] T. Chatpong and S. Paradorn, "Attitudes towards CAPTCHA: A Survey of Thai Internet Users," *The Journal of Global Business Management*, vol. 9, no. 2, 2013.

[32] A. F. Christos, M. A. Nikolaos and G. V. Artemios, "On the Necessity of User-Friendly CAPTCHA," BC, Vancouver, Canada, 2011.

[33] F. Anita, "Biometric Alternatives to CAPTCHA: Exploring Accessible Interface Options," 2012.

[34] M. a. Welie, G. V. D. Vee and A. Eliëns, "Breaking down usability," in *In Proceedings of INTERACT*, 2012.

[35] W. Nelson, W. Turin and T. Hastie, "Statistical methods for on-line signature verification," *IJPRAI*, vol. 8, no. 3, p. 749–770, 1994.

[36] J. Judy, "Usability assessment of academic digital libraries: Effectiveness, efficiency, satisfaction, and learnability," *International Journal of Libraries and Information Services*, no. 55, p. 96–121, 2005.

[37] R. Tuley, "How the textCAPTCHA web service works," 2012. [Online]. Available: http://textCAPTCHA.com/how_it_works. [Accessed 23 June 2012].

[38] C. Hernandez-Castro, A. Ribagorda and J. Hernandez-Castro, "THE STRENGTH OF EGGLUE AND OTHER LOGIC CAPTCHAs," SCITEPRESS (Science and Technology Publications, Lda.), Seville, Spain, 2011.

[39] B. Pfitzmann and M. Waidner, "Analysis of liberty single-sign-on with enabled Clients," *Internet Computing, IEEE*, vol. 7, no. 6, p. 38–44, 2003.

[40] G. Shin, A. Dongwan and P. Shenoy, "Ensuring information assurance in

federated identity management," in *Computing, and Communications, IEEE International Conference*, 2004.

[41] R. Gafni and I. Nagar, "CAPTCHA – Security Affecting User Experience,Issues in Informing Science and Information Technology," Informing Science Institute, Tel-Aviv, Israel, 2016.

APPENDIX

Questionnaire on university student's attitudes towards CAPTCHA

Section1 : Demographic Information:

1.	**Gender**	○ Male ○ Female
2.	**Age Category**	○ 16 - 20 ○ 21 - 25 ○ 26 - 30 ○ 31 - 35 ○ 36 - 40 ○ above 40
3.	**Education level**	○ Bachelor degree ○ Master degree ○ PhD degree

4. What is your department?

○ .....

5.For how long have you been using internet?

○ Less than 3 years ○ 3 to 5 years ○ 6 to 9 years ○ 10 years and more

6. How often do you use the internet?

○ Every day ○ 3 - 4 days a week ○ 5 - 6 days a week ○ less than once a week

Section2: Overall attitudes towards CAPTCHA

Please Indicate your agreement level to the following statements.

		I totally agree 1	2	3	4	I totally disagree 5
1.	**Using CAPTCHA is beneficial**	○	○	○	○	○
2.	**Using CAPTCHA is important**	○	○	○	○	○
3.	**CAPTCHA is enough to verify that the user is human**	○	○	○	○	○
4.	**CAPTCHA is credible**	○	○	○	○	○
5.	**CAPTCHA is comfortable**	○	○	○	○	○
6.	**I do not prefer website that use CAPTCHA**	○	○	○	○	○
7.	**CAPTCHA is a waste of time**	○	○	○	○	○
8.	**CAPTCHA is frustrating**	○	○	○	○	○

9.	**I prefer easy CAPTCHA even if it is less secure**	○	○	○	○	○
10.	**I do not trust websites without CAPTCHA**	○	○	○	○	○
11.	**I would not enter my personal information to websites without CAPTCHA**	○	○	○	○	○
12.	**I would not enter payment information to websites without CAPTCHA**	○	○	○	○	○
13.	**Overall, I believe CAPTCHA is needed to an enhance website and information security.**	○	○	○	○	○

Section3: Attitudes towards CAPTCHA types :

Part A: CAPTCHA Evaluation (Picture Based)

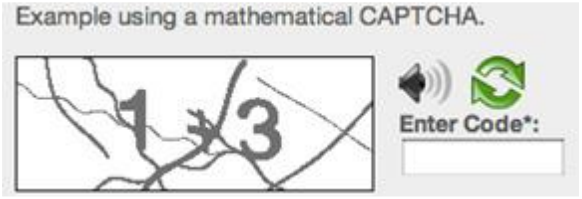
		I totally agree 1	2	3	4	I totally disagree 5
1.	**I am familiar with this type of CAPTCHA**	○	○	○	○	○
2.	**I believe that this type of CAPTCHA is easy to use**	○	○	○	○	○
3.	**I think that this type of CAPTCHA provides enough security**	○	○	○	○	○
4.	**This type of CAPTCHA is enjoyable**	○	○	○	○	○
5.	**This type of CAPTCHA is friendly and helpful**	○	○	○	○	○
6.	**This type of CAPTCHA can be suitable for all users**	○	○	○	○	○

7.	The performed task from this CAPTCHA is easy to understand	○	○	○	○	○
8.	This type of CAPTCHA does not requires a lot of time	○	○	○	○	○
9.	This type of CAPTCHA does not requires a lot of mental effort	○	○	○	○	○
10.	It is more possible not to make errors using this CAPTCHA	○	○	○	○	○

Part B: CAPTCHA Evaluation (Text Based)

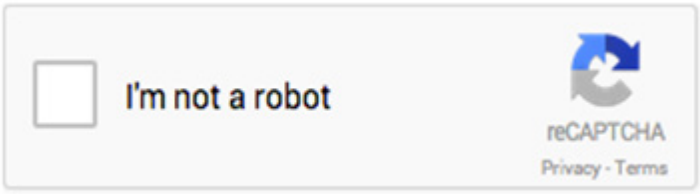
		I totally agree				I totally disagree
		1	2	3	4	5
1.	I am familiar with this type of CAPTCHA	○	○	○	○	○
2.	I believe that this type of CAPTCHA is easy to use	○	○	○	○	○
3.	I think that this type of CAPTCHA provides enough security	○	○	○	○	○
4.	This type of CAPTCHA is enjoyable	○	○	○	○	○
5.	This type of CAPTCHA is friendly and helpful	○	○	○	○	○
6.	This type of CAPTCHA can be suitable for all users	○	○	○	○	○
7.	The performed task from this CAPTCHA is easy to understand	○	○	○	○	○
8.	This type of CAPTCHA does not requires a lot of time	○	○	○	○	○
9.	This type of CAPTCHA does not requires a lot of mental effort	○	○	○	○	○
10.	It is more possible not to make errors using this CAPTCHA	○	○	○	○	○

Part C: CAPTCHA Evaluation (Arithmetic operation CAPTCHA)



		I totally agree 1	2	3	4	I totally disagree 5
1.	I am familiar with this type of CAPTCHA	○	○	○	○	○
2.	I believe that this type of CAPTCHA is easy to use	○	○	○	○	○
3.	I think that this type of CAPTCHA provides enough security	○	○	○	○	○
4.	This type of CAPTCHA is enjoyable	○	○	○	○	○
5.	This type of CAPTCHA is friendly and helpful	○	○	○	○	○
6.	This type of CAPTCHA can be suitable for all users	○	○	○	○	○
7.	The performed task from this CAPTCHA is easy to understand	○	○	○	○	○
8.	This type of CAPTCHA does not requires a lot of time	○	○	○	○	○
9.	This type of CAPTCHA does not requires a lot of mental effort	○	○	○	○	○
10.	It is more possible not to make errors using this CAPTCHA	○	○	○	○	○

Part D: CAPTCHA Evaluation (No CAPTCHA reCAPTCHA)



		I totally agree 1	2	3	4	I totally disagree 5
1.	I am familiar with this type of CAPTCHA	○	○	○	○	○
2.	I believe that this type of CAPTCHA is easy to use	○	○	○	○	○
3.	I think that this type of CAPTCHA provides enough security	○	○	○	○	○
4.	This type of CAPTCHA is enjoyable	○	○	○	○	○
5.	This type of CAPTCHA is friendly and helpful	○	○	○	○	○
6.	This type of CAPTCHA can be suitable for all users	○	○	○	○	○
7.	The performed task from this CAPTCHA is easy to understand	○	○	○	○	○
8.	This type of CAPTCHA does not requires a lot of time	○	○	○	○	○
9.	This type of CAPTCHA does not requires a lot of mental effort	○	○	○	○	○
10.	It is more possible not to make errors using this CAPTCHA	○	○	○	○	○

Part F: CAPTCHA Evaluation (Game based CAPTCHA)

	I totally agree 1	2	3	4	I totally disagree 5
1. I am familiar with this type of CAPTCHA	○	○	○	○	○
2. I believe that this type of CAPTCHA is easy to use	○	○	○	○	○
3. I think that this type of CAPTCHA provides enough security	○	○	○	○	○
4. This type of CAPTCHA is enjoyable	○	○	○	○	○
5. This type of CAPTCHA is friendly and helpful	○	○	○	○	○
6. This type of CAPTCHA can be suitable for all users	○	○	○	○	○
7. The performed task from this CAPTCHA is easy to understand	○	○	○	○	○
8. This type of CAPTCHA does not requires a lot of time	○	○	○	○	○
9. This type of CAPTCHA does not requires a lot of mental effort	○	○	○	○	○
10. It is more possible not to make errors using this CAPTCHA	○	○	○	○	○