DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
SOUTHEAST UNIVERSITY

CSE4000: Research Methodology
Privacy and Cookies Analysis for Cyber Security

A dissertation submitted to the Southeast University in partial fulfillment of the requirements for the degree of BSc in Computer Science & Engineering

Submitted by

Khadija Sifat Tania   Saeema Binte Sattar   Ishrat Jerin Era
ID: 2015000000096   ID: 2015000000135   ID: 2015000000177

Supervised by

Dr. Al-Sakib Khan Pathan
Associate Professor, Department of CSE
Southeast University

Letter of Transmittal

December 26, 2018

The Chairman,
Department of Computer Science & Engineering,
Southeast University,
Banani, Dhaka.

Through: Supervisor, Dr. Al-Sakib Khan Pathan

Subject: Submission of CSE4000 Research Report.

Dear Sir,

We are submitting here with the research report on "Privacy and Cookies Analysis for Cyber Security". It was a great pleasure for us to work on such a captivating topic. By following the instruction of yours and fulfilling the requirement of the Southeast University, this research work has been performed.

We have prepared this report with our utmost earnestness and sincere effort. We request your approval of this research report partial fulfillment of our degree requirement.

Thank you.

Sincerely yours,   Supervisor:

_____   _____
Khadija Sifat Tania   Dr. Al-Sakib Khan Pathan
ID: 2015000000096   Associate Professor
Batch: 39   Department of CSE
Program: BSc in CSE   Southeast University

_____
Saeema Binte Sattar
ID: 2015000000135
Batch: 39
Program: B.Sc. in CSE

_____
Ishrat Jerin Era
ID: 2015000000177
Batch: 39
Program: BSc in CSE

Certificate

This is to certify that the research paper titled "Privacy and Cookies Analysis for Cyber Security" is the bona-fide record of research work done by Khadija Sifat Tania, Saeema Binte Sattar and Ishrat Jerin Era for the partial fulfillment of the requirements for B.Sc. in Computer Science & Engineering (CSE) from Southeast University. This paper was carried out under my supervision and is record of the bona-fide work carried out successfully.

Author:

_____
Khadija Sifat Tania
ID: 2015000000096
Batch: 39
Program: B.Sc. in CSE

_____
Saeema Binte Sattard
ID: 2015000000135
Batch: 39
Program: B.Sc. in CSE

_____
Ishrat Jerin Era
ID: 2015000000177
Batch: 39
Program: B.Sc. in CSE

Approved by the Supervisor:	**Approved by the Chairman:**
_____	_____
Dr. Al-Sakib Khan Pathan	Dr. Al-Sakib Khan Pathan
Associate Professor	Chairman
Department of CSE	Department of CSE
Southeast University	Southeast University

Abstract

The present Internet sites are created with functionalities that allow website owners to track activities of website users. One of the systems by which websites perform the tracking is through cookies. Some of this cookies are third-party cookies that can track the user activities. This paper present an analysis how cookies become privacy concern for cyber security and estimated percentage of cookies of different websites. Also the rate at which third-party cookies are being set and probability of third-party cookies which can track user information or activities. We go through data privacy status of selective countries, among them we found some countries have no data privacy law. Finally, we suggested some ideas for data privacy to ensure cyber security.

Acknowledgement

At First and above all, we want to acknowledge the almighty Allah who providing us this opportunity and granting us the capability to complete our research work and finally finished researching a report without any trouble. we are appreciate to our respected supervisor Dr. Al-Sakib Khan Pathan, Associate Professor Department of CSE whose warm encouragement, thoughtful guidance and effective suggestion helped us to complete this work successfully.We want to acknowledge our most affectionate and dearest parents for their support and encouragement. We would like to thank our entire course-mate in Southeast University, who took part in any kind of discussion while completing this work.

Contents

List of Figures

Chapter 1

Introduction

Basically websites cookies are used to improve the browsing âexperience on frequently-visited websites. But now-a-days âcookies are also used to deliver many types of targeted digital marketing. They store user data and behavior information, which allows advertising services to target audience. Today, cookies are one of the main mechanisms that advertising companies like Google use to track and profile users across sites and over time often building up a single broad profile for years and years. But it turns out that the cookie situation is quite a bit trickier now, and sites that want to track users have new technical options that are hard for users to respond to.[5] Since the inception of cookies there has been an on-going discussion about the storage of âpersonal data and privacy, and in 2012 legislation was passed in the EU requiring every âwebsite which uses cookies to ask the users permission to store and retrieve data about them. [7] A survey by Pew Research revealed that 76 percent of respondents were concerned about privacy and security of records of their activities maintained by online advertisers. Tracking of users without consent is in general considered as a violation of usersâ privacy.[4]

In this paper, we report result of study estimated percentage of cookies of different websites. Also the rate at which third-party cookies are being set and probability of third-party cookies which can track user information or activities. In this paper, we also present a study on data privacy law status of selective

countries, among them we found some countries have no data privacy law. Finally, we suggested some ideas for data privacy to ensure cyber security.

1.1 Objective

The main objective of the research is that how cookies can effect in our privacy and how cookies track user information. Different types of websites collect data for different purpose. We want to clarify that data privacy is very important for cyber security. Our research will give an idea about which type of websites collect what type of cookies and it will suggest some ideas for data privacy to ensure cyber security.

1.2 Motivation

In this technological era internet is a great platform where people from all over the world can share and get information. Inspite of all the benefits that come with the internet, it has come at a cost that there is a chance to lose our privacy. Depending on the website and service we share different types of data, and the browser use the way âcookies policyâ to collect data. Most of the people are not aware about cookies that can collect user information and keeps tracks of all the browsing information and this is used by hackers and companies to know all our personal details like bank account details, user credit card information etc. which is dangerous . So we are interested to work on this topic.

1.3 Scope of Research

Our research is focused on analyzing cookies and data privacy relation. We identify most vulnerable cookie and analyze the data privacy law status of some countries and we provide some ideas for those countries which have no data privacy law. So that people can be aware about cookie.

Chapter 2

Literature Review

To the best our knowledge, some security agencies and people analyze about internet cookies. In 2011, European network and information security agency (ENISA) studies are required to identify to what extent the new Cookies can be used for tracking and their research takes into consideration the new types of cookies now being deployed in the online environment [8]. We go through some works on cookies related work and related on privacy control by cookie management and also Evaluation of Cookies-Setting Websites with Privacy Protection Laws and so on. We took some ideas from them and applied in our research. As our research is different from them in context through we took some ideas how to approach to the goal.

Chapter 3

Requirement of the Research

We analyzed first party and third party cookies from four different websites of different countries.

Generally first-party cookies are allowed in every Web browser but third-party cookies could keep track of user activity as they move from page to page. We use estimation process for calculating percentage of First party cookies and Third party cookies. We also use probability method for estimation of probability of user being tracked.

Chapter 4

Research Overview

4.1 Cookies

A cookie is a message given to an internet browser by a web server. The browser stores the message in a text file. The message is then sent back to the server each time the program asks for a page from the server. For example, Login information is stored in a cookie so the user can enter and leave the website without having to re-enter the same authentication information over and over.[21]

4.2 Types of Cookies

There are different types of cookies, But main type of cookies are:

- First-party cookies

First Party Cookies are written by website and can only be read by the website.

- Third-party cookies

Third Party Cookies are installed by third parties with the aim of collection certain information. They gather data about your browsing habits, and allow them to track you across multiple websites.

- Session cookies

Session Cookies are not actually written to a file but are stored in the browser itself. These cookies only last as long as the browser is open. Theyâre used for example on e-commerce websites so you can continue browsing without losing what you put in your cart.

- Persistent cookies

If session cookie contains an expiration date, it is considered as persistent cookie. On the date specified in the expiration, the cookie will be removed from the disk.

4.3 Cookies and Privacy Relation

Basically Cookies use to customize website, but third party cookies may related with privacy, Third-party cookies are known as marketing or tracking cookies. These are the cookies embedded by third-party websites. For example, advertisements and banners shown on a website user visit are usually displayed by a third-party. Google, Facebook, YouTube, and Twitter are some of the most common websites using third-party cookies.[9] We should keep in mind that anything personal could be saved into cookies, for example, credit card details, e-mail address and more. This means that if the cookies arenât sent over HTTPS, theyâre readable by anyone on the network. Any hacker connected to the same network can then use a sniffing tool (a software that intercepts traffic on a network) and steal all your sensitive data. Some people mistakenly believe that cookies are some kind of malware. They arenât, but they can be privacy concern because they can be used as spyware.[10] Many antivirus programs today will flag suspicious spyware or adware cookies when scanning user system for viruses.[11]

When tracking cookies can be seen by a malicious attacker, the cookies effectively moved toward becoming spyware. Spyware is software that is downloaded onto our computer to track our activities without our knowledge. This data is then sent to a remote source. The tracking cookies would then be able to be utilized to follow the user's activities on a site and target them in a social engineering attack or, depending on what is tracked, identity theft.

As cookies are transmitted back and forth between a browser and website, if an attacker or unauthorized person gets in between the data transmission, the sensitive cookie information can be intercepted. Although relatively rare, this can happen if the browser is connecting to the server using an unencrypted network like an non-secured WiFi channel.[12] Tracking of users without consent is in general considered as a violation of usersâ privacy

4.4 Selected Countries

We choose these countries because these countries are under top 20 countries with the highest number of internet user and we have selected three Asian countries and three European countries.// Our selected countries are:

- Bangladesh

- Japan

- China

- United Kingdom

- Germany

- Italy

4.5 Types of Website

We randomly selected these websites:

- E-commerce Website

- E-government Website

- Newspaper Website

- Blogging Website

4.6   Data Privacy Law Status

Information privacy law or data protection laws prohibit the disclosure or misuse of information about private individuals. Over 80 countries and independent territories, including nearly every country in Europe and many in Latin America and the Caribbean, Asia, and Africa, have now adopted comprehensive data protection laws.[1] The European Union has the General Data Protection Regulation[2], in force since May 25, 2018. [13] We selected six countries for our research purpose. There are three countries from Asia and three countries from Europe. The data privacy law of those countries are different from one another depending on the situations and issues of individual countryâs circumstances. According to UNCTAD, as of April 2018, only 58 percent of countries of worldwide estimation have data protection laws and 10 percent have draft laws. However, this still leaves nearly 21 percent of countries with no laws in place. In this year there are 45 percent of Asian countries have data privacy laws, 7 percent have draft laws, 32 percent have no laws and 17 percent have no data to conduct laws. From European countries there are 98 percent countries have data protection law and surprisingly only 2 percent have no data[14].

The Data Protection Act controls how a userâs personal information is used by organizations, businesses or the government. Everyone is responsible for using personal data has to follow strict rules called 'data protection principles'. They should ensure the data is utilized decently, legitimately and straightforwardly.

4.7 Data Privacy Law Status of Our Selected Countries

Bangladesh:

According to UNCTAD, as of April 2018, only 58 percent of countries of worldwide estimation have data protection laws and 10 percent have draft laws. However, this still leaves nearly 21 percent of countries with no laws in place. Still Bangladesh is on the country list of no data protection law.[14]

Data Protection Law Status of Bangladesh:

Electronic Transactions:

Legislation

Consumer Protection:

Legislation

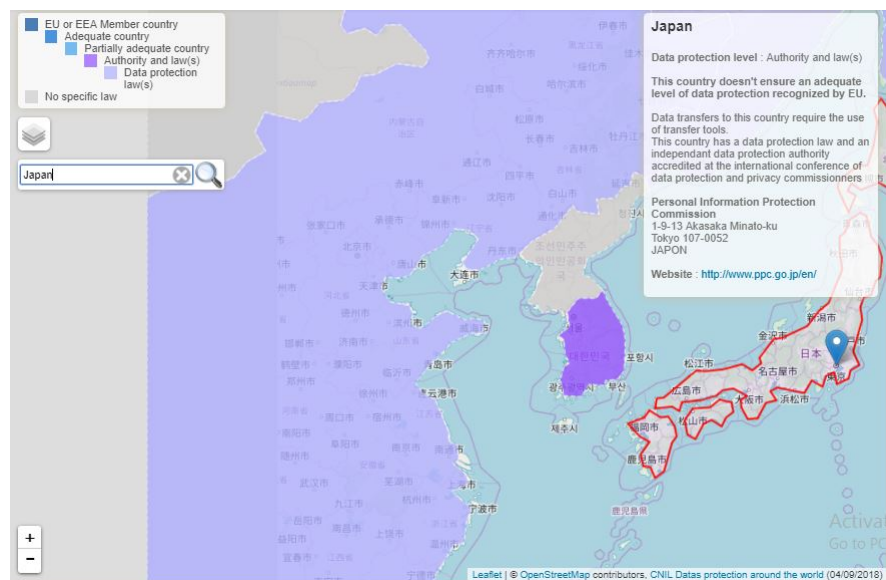Privacy and Data Protection:

No Data

Cybercrime: Legislation
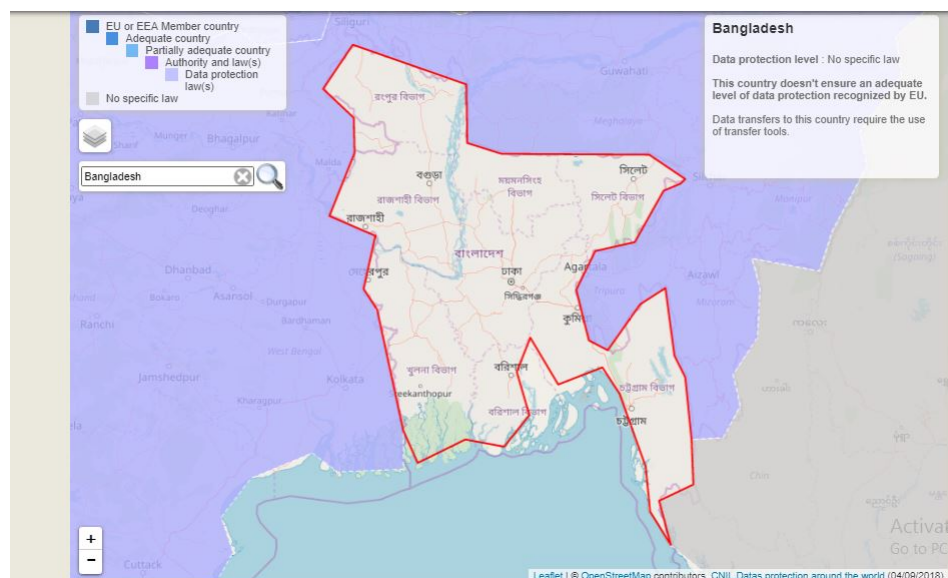
Figure 4.1: Data Protection Law Status of Bangladesh

Japan:

Japan is not an EU Member State and therefore has not implemented the GDPR or the Data Protection Directive. However, the Act on the Protection of Personal Information (Act No. 57 of 2003) (the âAPPIâ) contains similar provisions. An act to amend the APPI (the âAPPI Amendmentâ) came into force fully on 30 May 2017. References in this summary to the APPI Amendment indicate the changes made by the amendment.[16].

Data Protection law status of Japan:

Electronic Transactions:

Legislation

Consumer Protection:

No Data

Privacy and Data Protection:

Legislation

Cybercrime: Legislation

Figure 4.2: Data Protection Law Status of Japan

CHAPTER 4. RESEARCH OVERVIEW

China:

Laws regulations database of the republic of china is the website of china data privacy law.Ministry of Justice last time amended the law at 30th December 2015.The principal personal data privacy law in china is cyber security law of peoplesâ republic (CSL).It sets out data protection requirements for network operators. There are civil and criminal laws that have impact on data protection. Under the cyber security law the Cyberspace Administration of china (CAC) is responsible for planning and coordination of cyber security and relevant supervisory administration work[15].

Data Protection Law Status of China:

Electronic Transactions:

Legislation

Consumer Protection:

Legislation

Privacy and Data Protection:

Legislation

Cybercrime:

Legislation

Figure 4.3: Data Protection Law Status of China

Italy:

The Italian Board of the Ministries has approved the final text of Italian privacy law integrating the GDPR. This has raised major concerns on the scope of the law. On the 8th of August 2018, the Italian Board of Ministries announced that they have approved the Italian privacy law integrating the GDPR. The General Data Protection Regulation (EU) 2016/679("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).[20]

Data Protection Law Status of Italy:

Electronic Transactions:

Legislation

Consumer Protection:

Legislation

Privacy and Data Protection:

Legislation

Cybercrime: Legislation

Figure 4.4: Data Protection Law Status of Italy

United Kingdom:

ICO is the Information Commissioners office of UK.The UKâs independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Data Protection Act (DPA) 2018 The UKâs DPA 2018 (Data Protection Act 2018) supplements the EUâs GDPR (General Data Protection Regulation) by filling in sections of the Regulation that are left to individual member states to interpret and implement. The DPA 2018 also applies âa broadly equivalent regimeâ â which it calls âthe applied GDPRâ â to certain types of personal data processing that fall outside the GDPRâs scope. These include processing for law enforcement purposes and processing by public authorities. Because the DPA 2018 supports the GDPR rather than enacting it.

Data Protection law of United Kingdom:

Electronic Transactions:

Legislation

Consumer Protection:

Legislation

Privacy and Data Protection:

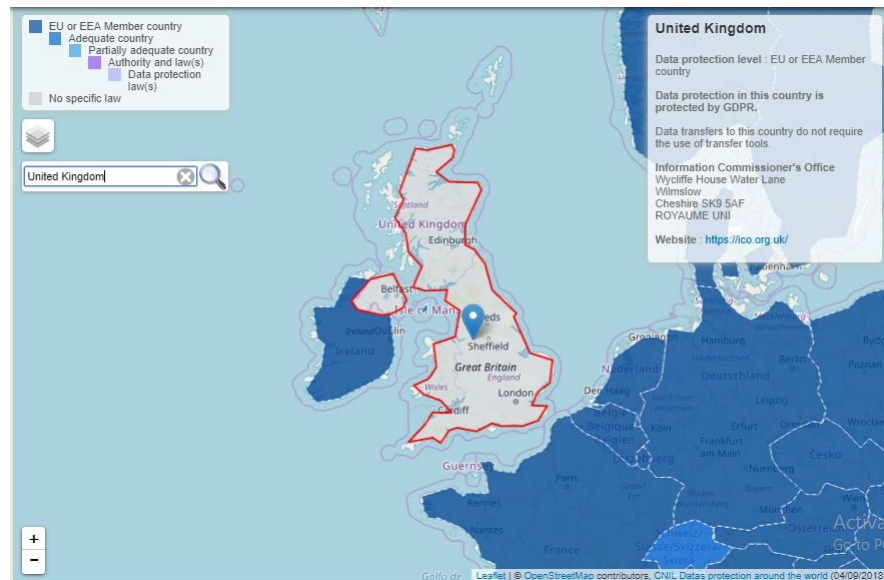Legislation

Cybercrime:

Legislation

Figure 4.5: Data Protection Law Status of United Kingdom

.

Germany:

The Federal Commissioner for Data Protection and Freedom of Information (die bundesbeauftragte fur den datenschutz und die informationsfreiheit) is the website for Germany data protection law. General data protection regulation (DS-GVO) is applicable from 25th may, 2018.It regulated the handling of personal data in European Union. Central data point (ZASt) explains the central data point. It coordinates the German data protection supervisory authorities from federal and state governments in the European data protection committee. European data protection board (EDSA) is created by GDPR and coordinates with it. The BfDI secures and develops data protection as highest federal authority. It controls and advise all public federal sector bodies and also nonpublic bodies. Freedom of information grants every citizen the right of free access of official information of public agencies of confederation and access to their administrative

procedures [18].

Data Protection law of Germany:

Electronic Transactions:

Legislation

Consumer Protection:

Legislation

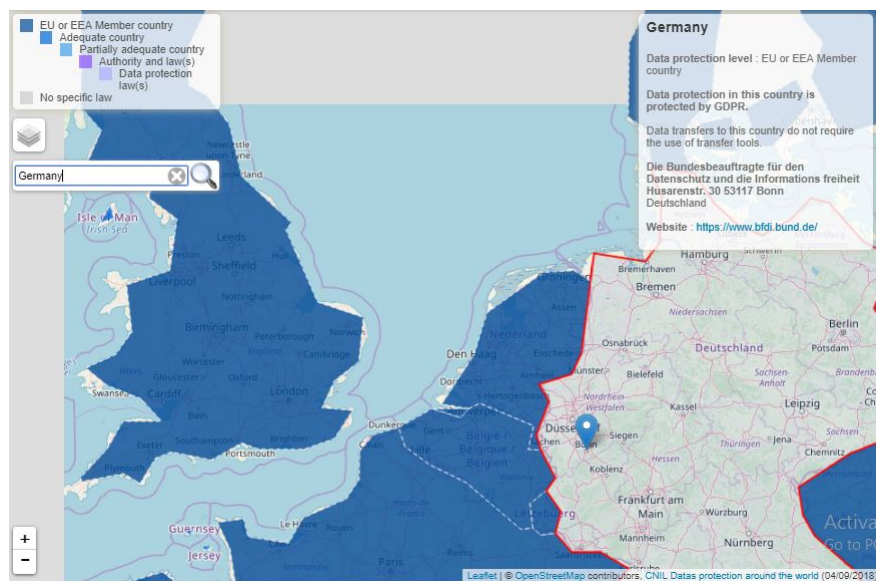Privacy and Data Protection:

Legislation

Cybercrime:

Legislation

Figure 4.6: Data Protection Law Status of Germany

.

Chapter 5

Implementation

5.1 Data Collection

Country	E-commerce				E-government				Newspaper				Blogging				Total			
	N	FP	TP	BP	N	FP	TP	BP	N	FP	TP	BP	N	FP	TP	BP	N	FP	TP	BP
Bangladesh	10	10	8	8	10	0	0	0	10	8	6	4	10	4	4	3	40	22	18	15
Japan	10	10	8	8	10	8	4	4	10	10	10	10	10	10	5	5	40	38	27	27
China	10	7	7	5	10	0	0	0	10	9	7	6	10	9	6	5	40	25	20	16
UK	10	10	9	9	10	10	9	9	10	10	9	9	10	10	7	7	40	40	34	34
Germany	10	9	7	5	10	10	3	3	10	9	8	7	10	9	9	8	40	37	27	23
Italy	10	10	10	10	10	10	7	7	10	9	9	9	10	10	10	10	40	39	36	36
	60	56	49	45	60	38	23	23	60	55	49	45	60	52	41	38	240	201	162	151

Figure 5.1: Summary of cookies collected per category per country

Abbreviations used in Table :

- N - Number of websites analyzed in each category

- FP - Number of websites per category that set first-party cookies only.

- TP - Number of websites per category that set third-party cookies only.

- BP - Number of websites per category that set both first and third-party cookies.

The table shows the number of websites per category and the number of websites that set first-party and third-party cookies and both of them. The table shows a wide use of cookies by the selected websites across all categories.

5.2 Data Analysis

The cookies set by websites in our selected countries are summarized in Table 5.1. So here is the calculation:

Total No. of websites, N=240

$$\text{Set of cookies} = \frac{218}{240} * 100$$

$$= 90.83\%$$

$$\text{Set first party cookies, FP} = \frac{201}{240} * 100$$

$$= 83.75\%$$

$$\text{Set third party cookies, TP} = \frac{162}{240} * 100$$

$$= 67.5\%$$

$$\text{Set first party \& third party cookies, BP} = \frac{151}{240} * 100$$

$$= 62.91\%$$

Out of the total of 240 analyzed websites, 218 (about 91%) of the websites set cookies, and 218 out of 240 (about 84%) set first-party cookies and (about 68%) set third-party cookies and (about 63%) also set both first-party and third-party cookies. The analysis also revealed that E-Commerce and Newspaper websites set significantly more third-party cookies.The estimation is shown in Figure 5.2
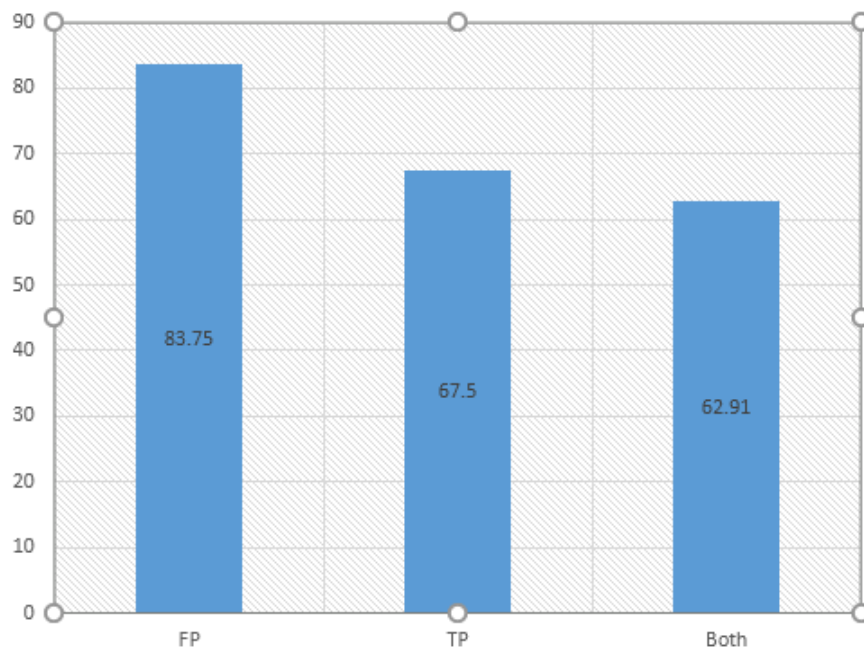
Figure 5.2: Estimated percentage of first-party,third-party and both cookies

Probability of use of third party cookies:

Bangladesh

Use of E-commerce website $=$ $= \frac{8}{10} * 100 = 80\%$

Use of E-government website $=$ $= \frac{0}{10} * 100 = 0\%$ [*Not applicable]

Use of Newspaper website $=$ $= \frac{6}{10} * 100 = 60\%$

Use of Blogging website $=$ $= \frac{4}{10} * 100 = 40\%$

Japan

Use of E-commerce website $=$ $= \frac{8}{10} * 100 = 80\%$

Use of E-government website $=$ $= \frac{4}{10} * 100 = 40\%$

Use of Newspaper website $=$ $= \frac{10}{10} * 100 = 100\%$

Use of Blogging website $=$ $= \frac{5}{10} * 100 = 50\%$

China

Use of E-commerce website $=$ $= \frac{7}{10} * 100 = 70\%$

Use of E-government website $=$ $= \frac{0}{10} * 100 = 0\%$ [*Not applicable]

Use of Newspaper website $=$ $= \frac{7}{10} * 100 = 70\%$

Use of Blogging website $=$ $= \frac{6}{10} * 100 = 60\%$

<u>United Kingdom</u>

Use of E-commerce website $= = \frac{9}{10} * 100 = 90\%$

Use of E-government website $= = \frac{9}{10} * 100 = 90\%$

Use of Newspaper website $= = \frac{9}{10} * 100 = 90\%$

Use of Blogging website $= = \frac{7}{10} * 100 = 70\%$

<u>Germany</u>

Use of E-commerce website $= = \frac{7}{10} * 100 = 70\%$

Use of E-government website $= = \frac{3}{10} * 100 = 30\%$

Use of Newspaper website $= = \frac{8}{10} * 100 = 80\%$

Use of Blogging website $= = \frac{9}{10} * 100 = 90\%$

<u>Italy</u>

Use of E-commerce website $= = \frac{10}{10} * 100 = 100\%$

Use of E-government website $= = \frac{7}{10} * 100 = 70\%$

Use of Newspaper website $= = \frac{9}{10} * 100 = 90\%$

Use of Blogging website $= = \frac{10}{10} * 100 = 100\%$
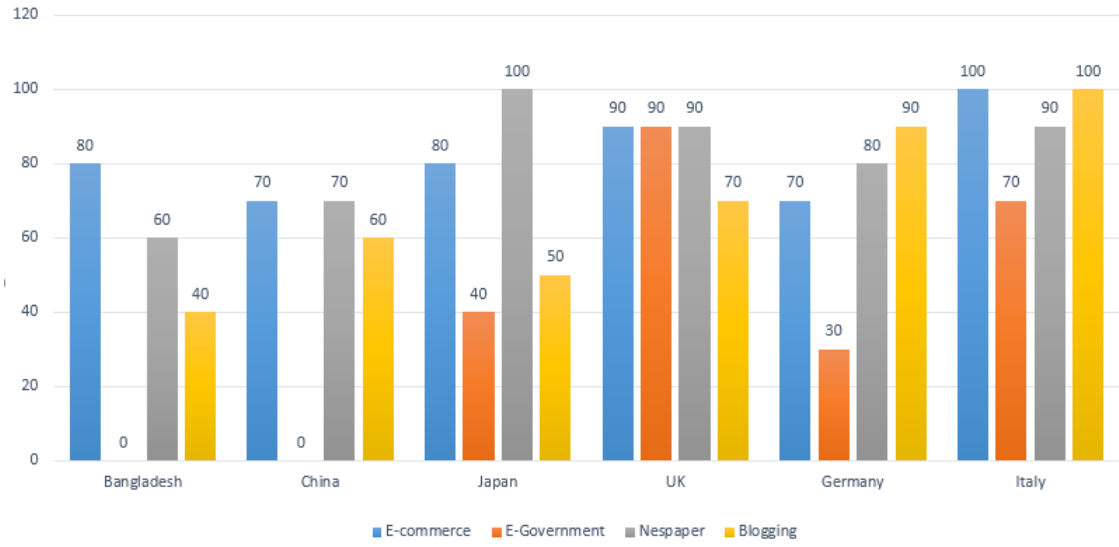
Figure 5.3: Estimation of third-party cookies for selected countries

$$\text{Bangladesh} = \frac{18}{162} = 0.11$$

$$\text{Japan} = \frac{27}{162} = 0.16$$

$$\text{China} = \frac{20}{162} = 0.12$$

$$\text{United Kingdom} = \frac{34}{162} = 0.20$$

$$\text{Germany} = \frac{27}{162} = 0.16$$

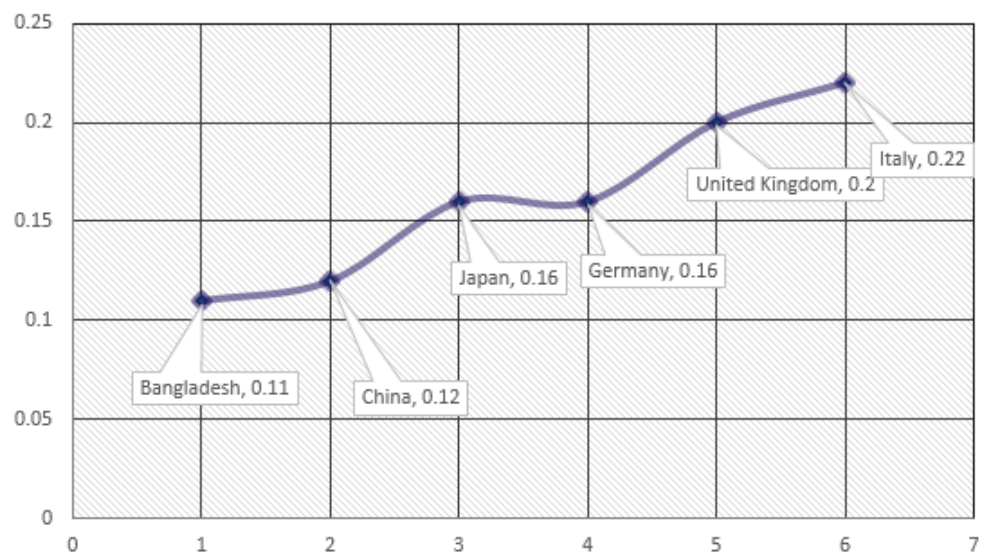$$\text{Italy} = \frac{36}{162} = 0.22$$

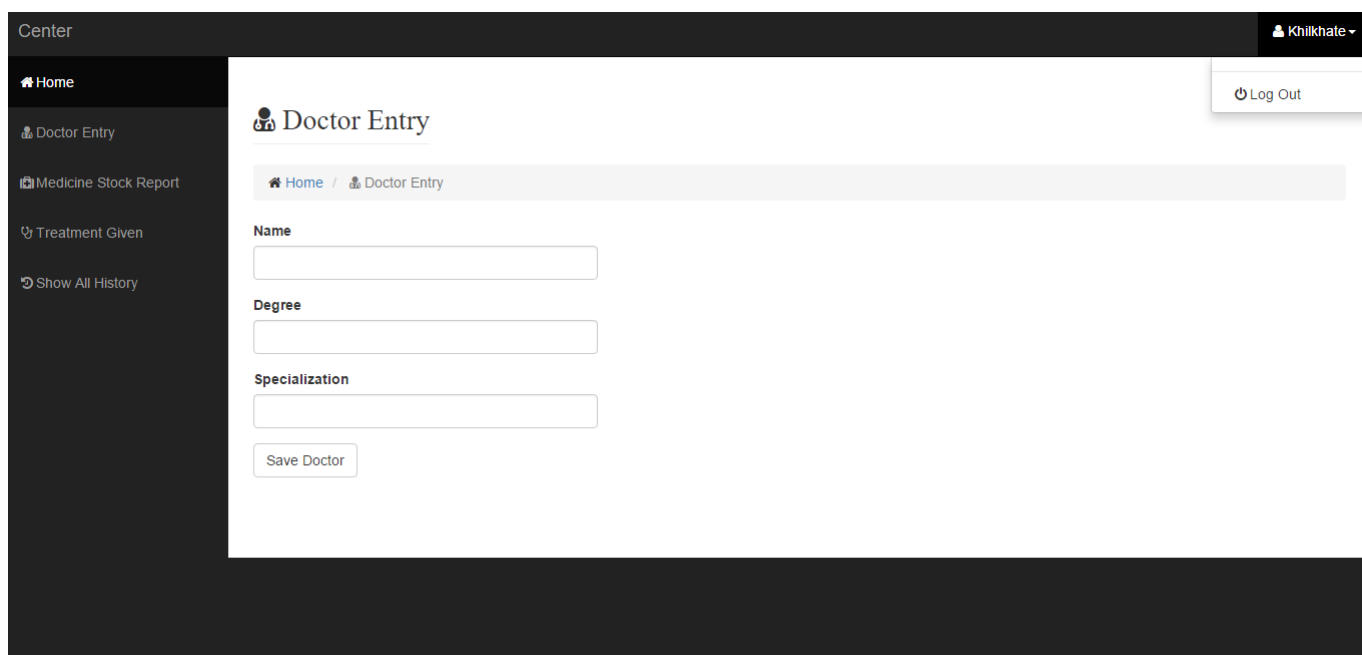Figure 5.4: Estimated probability of user being tracked

Chapter 6

Result and Decision

6.1 Result

After analyzing data we found that E-Commerce websites and Newspaper websites set more third-party cookies than E-government and Blogging websites and we also get the probability of use of third-party cookies.

On that estimation of probability, it shows the tracking probability by third-party cookies of Italy is high.

Figure 6.1: Center login Successfully

This is the view of Center login and then log out, return back to the center login page.

Figure 6.2: Medicine Entry Successfully

Medicine Entry successfully. This medicine will show to the all center.
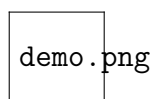

Figure 6.3: Demographic Mapping Report

District area wise and population wise, patient history shows in mapping, mouse cursor turning and its hover to treatment details.

Figure 6.4: Treatment given

Doctor input all information and then click to add, doctor all information view. When saving, that is the prepare to e-prescription.

Chapter 7

Conclusion

7.1 Conclusion

Guarantor for the protection of personal data is the website of Italian Data Protection Law

automation has great prospect of providing significant enhancement and cost effectiveness and better quality of medical to the within privileged rural, semi rural and downtown population. If we include community medical support in existing well being centers, then it will be easier and cheaper to produce health care for the people in remote areas.By supplying emergency services, it could possibly reduce the pressure of good sized quantities of patients in a reputed hospital.Government and other non-public organizations come forward to purchase community medicine, automation sector to ensure community medicine can serve medical service to remote people and generate new sources regarding employment.

7.2 Future Work

Our work is on community medicine automation services,so it has a vast opportunity of research. Our future work will be to make HCMA more cost effective,provide faster communication facilities,connect patient via video conferencing.we can expand community automation for getting better treatment and

follow-up by which we can ensure the foreign medical services and reduce the tendency of going abroad.

Bibliography