IMPACT OF RELATIONSHIPS ON RESPONSE TO SHOULDER SURFING

KINSHUK BHARDWAJ

School of Computing Science

Sir Alwyn Williams Building

University of Glasgow

G12 8RZ

A dissertation presented in partial fulfillment of the requirements of the Degree of Master of Science at the University of Glasgow

5th September 2019

TABLE OF CONTENTS

Acknowledgment

First, I would like to thank the Computing Science department and Dr. Mohamed Khamis, my thesis supervisor, who helped me throughout the project, offering me guidance through every step of my project by offering me valuable suggestions.

I would also like to thank all those who took part in my survey and study for my research and evaluation. I am also grateful to the.

I would also like to thank my parents and my friends for their constant support.

Section 1: Introduction

Shoulder surfing is a scenario where personal and/or private information is observed through the means of direct (directly looking) or indirect observation (for example: observing via reflections). It generally involves two or more individuals where one or multiple of them try to look over the other person's shoulder either consciously or unconsciously while the victim is totally unaware of the leak of his personal and private information and happens without his consent. Shoulder surfing is a common occurrence in day to day lives (according to the survey conducted during the thesis) which mostly occurs in open crowded places where the victim uses a portable device with a screen for display, for example, an ATM machine, a smartphone device or a computer. The ones occurring in public space are generally based out of curiosity and boredom ((Eiband et al., 2017). This can also occur in less crowded places which then may be classified as an act of intentional intrusion to invade the victim's privacy.

There have been various research conducted and work done in the field of shoulder surfing with most of the early works being in the year 2007 (Eiband et al., 2017). The objective of the thesis is to establish the impact of different types of relationships on the reaction of the people involved in shoulder surfing scenarios. Previous works have been conducted which shows that people have a sense of negative feeling in such scenarios (Eiband et al., 2017), but how do these reactions change if the relationship between shoulder surfer and the victim changes is not explored. The thesis also tries to establish the relationship impact on the various proposed privacy protection and alerting mechanisms (for example dimming filter mask, crystallize filter, fake text, vibrating alert, low brightness, etc. (Khamis, Eiband, et al., 2018; Zhou et al., 2015; Saad et al., 2018; ACM SIGCHI, 2016)) and how does the preference of mechanism change with changing relationship between the shoulder surfer and the victim. A small proof of concept of an android application has also been developed that detects the user's eyes and then tracks both eyes pupil and shows with some approximation if the user is looking left or right for each of the eyes.

According to the initial survey conducted, it became evident that people do not like if they are being shoulder surfed and would want some mechanism to protect their privacy in some way or the other. It also came into light that people react differently if they are shoulder surfing other or being shoulder surfed on if the relationship between the 2 individuals changed (one person being the shoulder surfer and the other being the victim). From now on in the thesis, the reference of the two mentioned individuals will be done as person A and person B, where person

A is the victim who is being shoulder surfed or the user of the device and the person B is the attacker or the shoulder surfer who tries to invade person A’s privacy without their consent.

Studying the impact of the relationships on the people’s reaction in shoulder surfing scenarios gave an insight into how they would want different protection mechanisms for different relationships. On the other hand, for some participants, the relationship was not a major factor influencing how they would react to being shoulder surfer. It was also evident from the initial survey that if some protection mechanism would have been present in the device being used by person A, then the person B would not have shoulder surfed person A at all. These results will enable to enhance the privacy protection mechanisms in case of shoulder surfing by improving the design and the way they would work in different scenarios and environments.

Section 2: Related Work

2.1 Research

Among the plethora of works studying shoulder surfing, (Eiband et al., 2017), in their paper, focused on finding the context, threat and risk implication of shoulder surfing scenarios on users in order to understand the feelings of individuals involved, the contents at risk during shoulder surfing, and how person A wants to protect their privacy and personal information when and if they are attacked. His findings suggest/highlighted important pointers that are to be considered while designing the various privacy protection mechanisms aimed to be deployed in public space (Eiband et al., 2017). It also showed that, while most of the users were unaware of being shoulder surfed (Eiband et al., 2017), most of them were unhappy on finding that their data was being observed without their consent. The common media to be observed were mostly, but not limited to, texts, pictures, and games (Eiband et al., 2017). Despite the finding that most of the participants acting as person B shoulder surfed only out of curiosity and had no malicious intent, they too experienced a negative feeling on realizing their unconsented act of invading person A's privacy.

Other works study possible situations and scenarios where the users' data is accessed, without authorization, and its consequences on the user (Marques et al., 2019). Different events recorded by (Marques et al., 2019) categorize the motivation of the attacker and the context of the attack. They also provide a qualitative analysis on how the trust and blame-game functions in shoulder surfing scenarios, which could in-turn weaken or in some cases even strengthen the relationship between the person A and B. One of the ways to control a smartphone would be with one's eyes. This could be especially helpful in shoulder surfing scenarios where person A would want to be subtle about protecting their content from being observed. (Majaranta & Bulling, 2014) studied eye movements and its use as an input method explaining its application in different environments. In addition, they also listed out potential issues that are associated with designing gaze-based interaction systems.

Other works trace the evolution of eye tracking on portable devices or hand-held devices and discuss the technical challenges faced within (Khamis, Alt, et al., 2018). (Khamis, Alt, et al., 2018) categorized the gaze interactions as gaze behavior, implicit gaze behavior, and explicit gaze behavior (sub-categorized into gaze-only and multimodal interactions). Using overlaid masks on the device's display, he presents ~~a~~ proof of concept for gaze-based interaction system that tracks/by tracking the user's eyes and displays the screen content only through two different sized circular spot, while everything around is either blacked out, distorted or covered by fake text (Khamis, Eiband, et al., 2018). A comparison of different hiding mechanisms indicated that the Crystallize filter was least stressful for users to read the text through while maintaining a high reading speed (Khamis, Eiband, et al., 2018).

Various other notification mechanisms such as blackout, selective showing (Zhou et al., 2015), alert icon, vibrating feedback (Saad et al., 2018), selective hiding and dim (ACM SIGCHI, 2016) have also been proposed that would alert the user in case of a possible shoulder surfing scenario. All these mechanisms have been included in the study evaluation for this thesis in terms of how one or more is prioritized over others depending on changing relationships between person A and B. The thesis also examines how the change in the relationship of person A and B would impact their feelings, reactions and consequences in shoulder surfing scenarios.

2.2 Software

The software solution involving the use of one's eyes are still in their early stages of development as none of them have reached their full potential, to begin with. The most notable among the available eye-tracking solutions use python as the development language, tracking pupils in real-time. It not only notifies if the user is looking left, right or straight but also displays the real-time coordinates for the pupils (Lamé, 2019). However, this software requires a computer with Python installed, as well as an external high-quality web camera which would display the direction of the user's gaze, and this very requirement makes it impractical to implement and run on a hand-held device such as an android based smartphone.

We focus mainly on Android-based smartphones as they are the leading operating system globally, occupying 74.45% in market shares as compared to Apple's iOS with 22.85% and others with 2.70%, as of January 2019 (Casserly, 2019). There have been some android based solutions that use eye gaze to detect if the user is safe and sound while driving (Flast, 2014). However, Flast warns that this application serves as a proof of concept only and has not been tested in real-life scenarios. On testing the application on the Android API level 28 and following the tutorial provided in the README file, the application did not work as claimed (android application link: https://bit.ly/2lsfuRW). Similarly, (horstlb, 2015, p.)'s application, which uses eye gestures to unlock the smartphone lock screen, failed to fulfill its claims on testing (android application link: https://bit.ly/2knseZN). (Matheus, 2017)it's software solution developed using C++ also uses an external webcam for live video feed which tracks the movement of the mouse on the desktop screen using open-source computer vision (OpenCV) library. After analyzing various available software solutions across platforms, this thesis provides for an android based eye tracking system that tells the user which direction each of their eyes are looking.

2.3 Own Contribution in Comparison to Prior Work

The work presented in this thesis primarily focuses on the relationship impact on the reaction and feelings of people on experiencing shoulder surfing scenarios. This takes forward the previous work done in knowing the general reactions of people at such times to classifying them into different types based on their relationships. Based on the feedback received from the initial survey about the features preferred by participants to avoid or be notified about a potential shoulder surfing scenario, an android based software solution is implemented and enhanced as a proof of concept to activate one of the many privacy protection mechanisms suggested in previous works. Furthermore, the privacy protection and notification mechanisms proposed in previous works are studied and analyzed in-depth with respect to different relationships and how people find them suitable in different situations.

Section 3: Methodology

3.1 Online Survey

The aim of this thesis is to understand the change in the impact of the relationships in people's reactions when they are involved in shoulder surfing situations, either as person A or as person B. To achieve this goal, the first step to that was to gather feedback from people about what do they feel about shoulder surfing and how do they react to being shoulder surfed along with understanding the minute details of their experiences either as person A or as person B or both. To move ahead with this, an online survey of a structured interview using a questionnaire was carried out to do the initial research on how people would react to shoulder surfing scenarios with changing relationships. This method was picked as it enabled a greater reach to get more responses which would help to get better results. The questions were framed in a way that there was no right or wrong answer but were open-ended questions which aimed at getting detailed information from the participants about their personal experiences. The online survey was divided into two sections, with the first comprising of open-ended questions regarding personal experiences of shoulder surfing and their reactions, while the second half of the survey focused on getting the demographic data of the participants like age, gender, current location, occupation, nationality, etc. The qualitative based feedback and demographic-based questions can be found inside the Online Survey Questions subdirectory of code.

The link to this initial survey could be found in Online Survey Link under code directory. The initial survey was conducted where 25 complete and 13 incomplete responses were received. The incomplete responses have not been taken into consideration at all in this thesis. Out of the 25 complete responses received, 10 were female, 14 were male, and one participant did not reveal their gender. The age range of the participants in the survey was in between 18 years old and 54 years old. 64% responses received were from students and others included doctors (8%), engineers (8%), homemakers (8%), barista worker (4%), musicians (4%), and service workers (4%). The pie charts showing the above statistics can be found in subdirectory Initial Survey Demographic statistics of code directory.

3.2 Android Application

The results from the initial survey led to an inference that most of the people are not comfortable with their data being watched over their shoulders and would prefer some kind of a mechanism that would help to protect their privacy, either on their smartphones or as a hardware solution, for example, a privacy protection screen. Hence, the next step was to devise software-based proof of concept solution using eye-tracking in android that the user could use to activate one of the privacy protection mechanisms proposed by (Zhou et al., 2015), (Saad et al., 2018), and in (ACM SIGCHI, 2016). This solution is discussed in detail in section 5.

3.3 Evaluation Study

Using this software solution to activate the proposed privacy protection mechanisms, final testing and evaluation were carried out with 15 participants where no demographic details were captured. This was not an online study but was done in person with each of the participants. This was done to have a better and a deeper understanding of their feedback and inputs about the relationship impact on their choice of privacy protection mechanisms and also detailed qualitative feedback from the testing of the android application developed as a proof of concept. Each of the participants was shown a series of 12 videos which showcased the 12 different mechanism's working in a real-life scenario and then asked to answer questions from 1 to 8 in the evaluation questionnaire and then question 9 and 10 at the end. Each of the questions from 1 to 8 was for different relationship and asked for the participants to rate each of the mechanisms shown one by one on a scale of 1 to 5 in terms of suitability, with 1 being the least suitable and 5 being the most suitable one. Question 10 was related to the testing and feedback of the proof of concept android application developed that tracked users' eye and displayed the direction in which each of their eyes was pointing at in real-time. The evaluation study-related instructions that were given to each participant can be found in the Evaluation Study Questionnaire under root while the questions are present in the same file. The results and feedback from this evaluation study are discussed in detail in section 6.

Section 4: Analysis and Requirements

4.1 Online Survey

The initial survey conducted for this thesis involved 25 responses from people of different age groups, background, and nationality. The results of the survey were collected in an excel sheet and grouped according to questions asked with rows as the number of participants and the columns having the various questions asked and other details like the time taken to answer each survey, the device used. The response sheet is also including the incomplete responses that were received. To filter out the incomplete responses, the rows were color-coded in a way that the incomplete responses have been marked as red in color while the complete responses as blue in color. The document link containing all the responses from the survey is in Shoulder_Surfing_Responses.xlsx under the directory code.

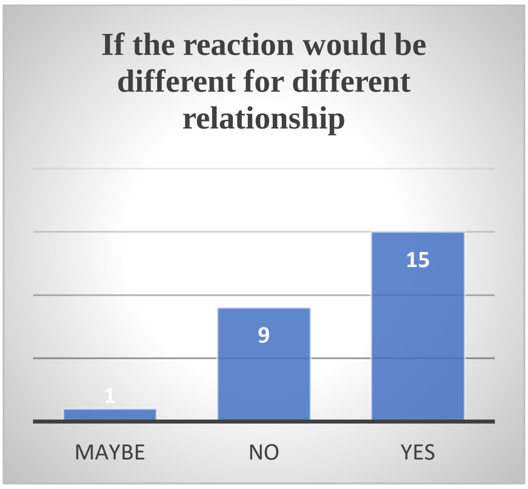
4.2 Online Survey Results

The initial response sheet was then thoroughly analyzed and summarized into information about participants' experience, time and place of event, the reactions of the people involved, parameters defining the why and if the change in the relationship would change their reactions and feelings, the content that person A was more interested in securing or which person B wanted to observe, the feature that could have been present in the device to prevent a shoulder surfing scenario, the device involved in the scenarios mentioned by the participants, and their gender and age. All this data was briefed into an excel sheet which was then used to analyze the various key points. This document link can be found in Initial Survey Summary.xlsx under code directory. 16 participants experienced a case of shoulder surfing as person A only (color-coded as blue in the document of Initial Survey Summary.xlsx under code directory) while 5 participants shared their experience as person B only (color-coded as red in the document of Initial Survey Summary.xlsx under code directory) and 4 participants recalled stories in which they acted as person A as well as the person B (color-coded as green in the document of Initial Survey Summary.xlsx under code directory).

All the participants acting as only person B were in a public space and mostly interested in a movie, video or game which person A was watching on their smartphone. 11 Participants acting as person A recalled that they were shoulder surfed while accessing personal and sensitive content on their phone. While 7 of the participants acting as person A claim that even though they were not accessing any sensitive content while being attacked by person B, yet they experienced a negative feeling of their privacy being invaded at that time. As person A, most participants had to look at person B which made person B to look away. Others acting as person A just took their own measures to prevent person B from observing their content by either tilting their screen away or had to change their screen. These results are in line with the findings of (Eiband et al., 2017)

4.3 Inference of Results

Next step was to analyze the effect of the change in the relationship in participant's reaction and feelings either as person A, person B or both. This was done by creating 2 separate sheets. one containing information about the participants' reaction, how and if they would have reacted differently if the relationship would have been different, the reason for a difference in their reaction and another sheet with the feelings they experienced, how and if they would have felt any differently if the relationship would have been different, and a probable reason for their change in feeling. The two sheets can be found in the document link attached in Initial Survey Summary.xlsx under code directory. After studying these inputs, the data revealed that 15 participants agreed that they would have reacted differently if their relationship would have been different, 9 claimed that their reaction would not have been any different and 1 participant was unsure of if they would react in a different manner with a change in their relationship (see figure 1 – left).



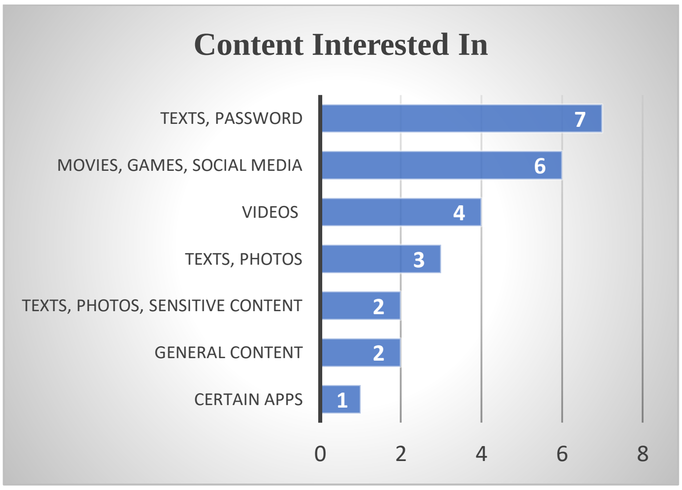
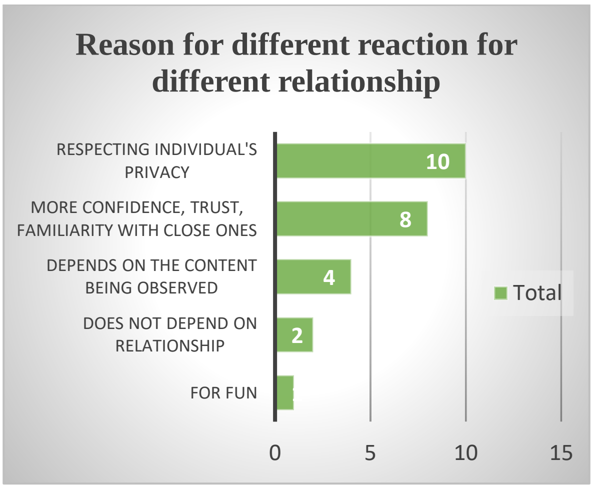


Figure 1: (LEFT) Chart depicting if the change in the relationship would impact the participant's reaction, (RIGHT) Graph showing commonly observed and leaked content during shoulder surfing scenarios

When asked to the participants about the reason for their change in their reactions, the most common reason was that an individual's privacy shall be respected at all points of time (10 responses) and that the trust and familiarity with known and close ones tend to be more (8 responses) and that. 4 participants said that their reaction would not only depend on the relationship but also on the content they are viewing at the time of shoulder surfing as person A. Other reasons included people doing it for fun (1 response) while few participants said that their reaction won't change with different relationships (see figure 2 – left). The most common content that was observed was texts and passwords, followed by movies, games, and social media, videos, photos, and sensitive content (see figure 1 - right).



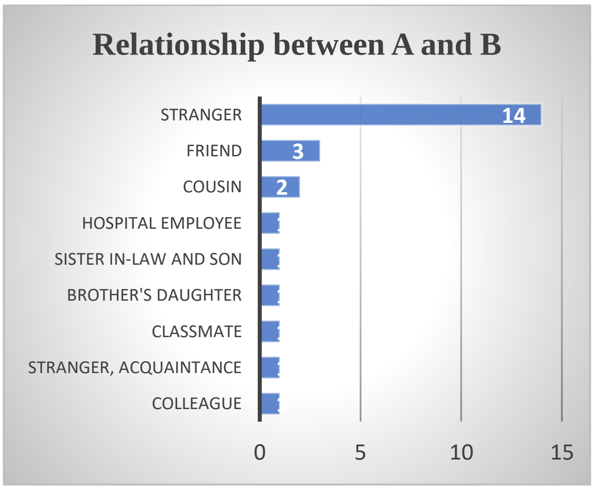


Figure 2: (LEFT) Graph showing the distribution of reasons for different reactions for different relationships, (RIGHT) Graph to show relationship mentioned by participants during their shoulder surfing experiences

Of all the experiences shared by the participants in the initial study, they encountered most of the shoulder surfing scenarios with strangers in public space. Some faced the situations with friends and family, while very few with office colleagues and classmates (see figure 2 – right).

It was revealed from the initial analysis that the feelings either as person A or as person B during shoulder surfing was mostly negative (see figure 3). Most of the participants acting as person A felt disturbed, uncomfortable or awkward when a person B observed their content without their consent. Participants irrespective of acting as A or B thought that privacy was being invaded in such cases. 5 participants did not experience any such feeling, neither negative nor positive. Most of the participants acting as person B was attracted to what was happening in person A's screen and found it interesting while some of them felt embarrassed about looking as A's screen.

There was a mixed response from the participants when asked if they would have felt different with a change in the relationship in their experience of shoulder surfing, as seen in figure 4 (right). It indicates that there were an equal number (12 each) of participants who yes and no to be above question, while just one participant was unsure if they would have felt differently in this scenario (see figure 4 – left). For the people who answered a yes to probably experiencing a different feeling if their relationship would change with the other person in the shoulder surfing scenario, the most common reason given was their comfort (6) and the trust (3) with their known and close ones. 4 participants felt the protection of privacy would be the major reason that would decide their feeling towards the other person. 1 participant did not answer this.

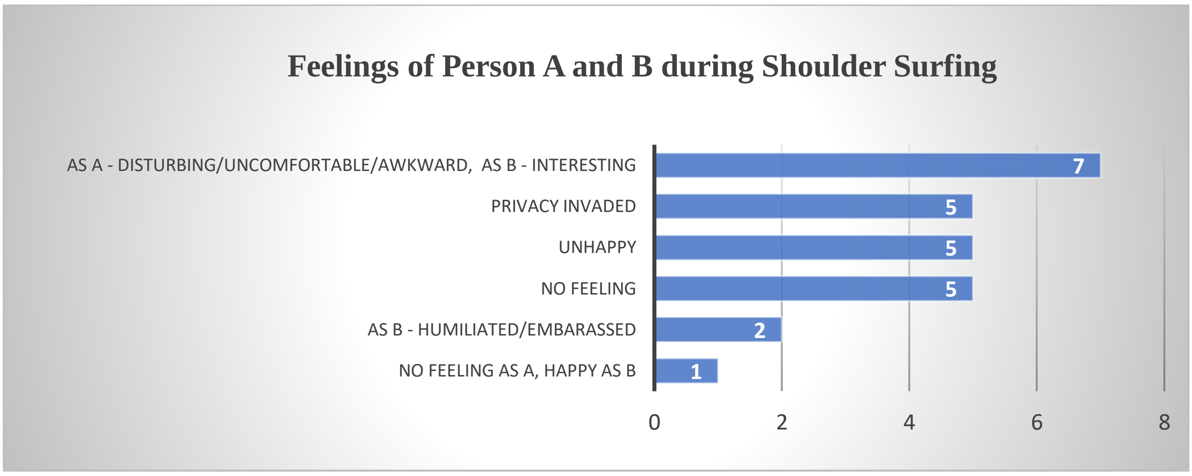


Figure 3: Graph showing how participants felt during shoulder surfing scenarios

After analyzing the survey data, it came into light that the most of the participants (6) wanted a software-based solution that could help prevent a shoulder surfing scenario or somehow indicate them as person A that such a scenario was possible that time (see figure 5). A similar number of participants (5) wanted a hardware-based solution, for example, a privacy screen guard to protect their privacy.

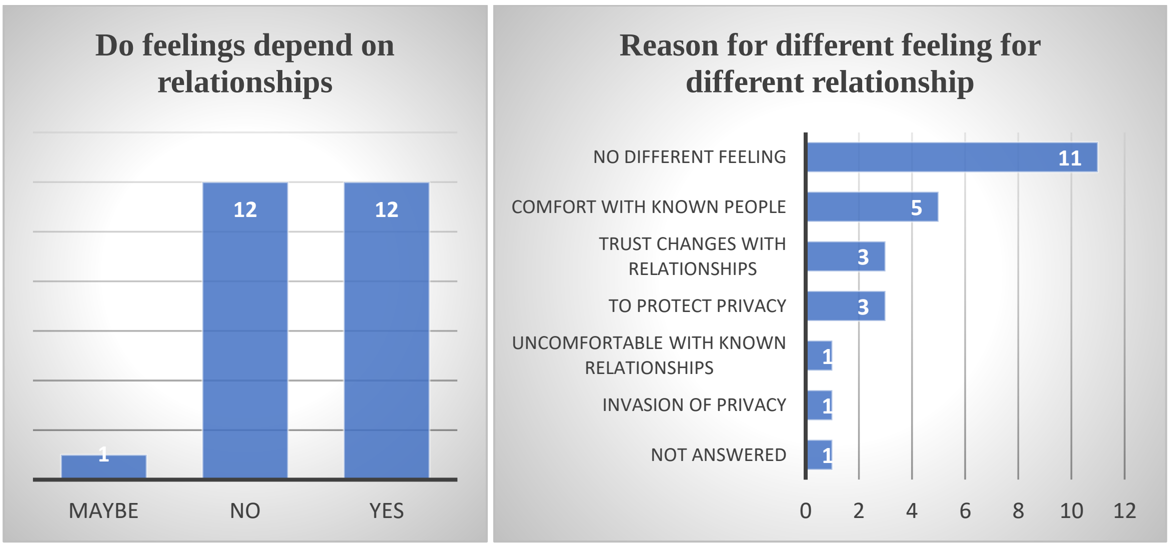


Figure 4: (LEFT) Graph showing if feeling change with changing the relationship, (RIGHT) Graph of different reasons for the change in feelings experienced with the change in relationship for participants

4 participants preferred if the device's viewing angle was reduced then people around them would not be able to observe content that person A would be accessing, and the same number of participants did not have an answer for such a solution. Other solutions suggested by participants included low brightness, and phone covers (like a flip cover to cover a side of the phone). 1 participant had a view that it was not possible for currently available technology to prevent a shoulder surfing scenario, but it always needs to come from the people in general who need to understand to respect the other's privacy.

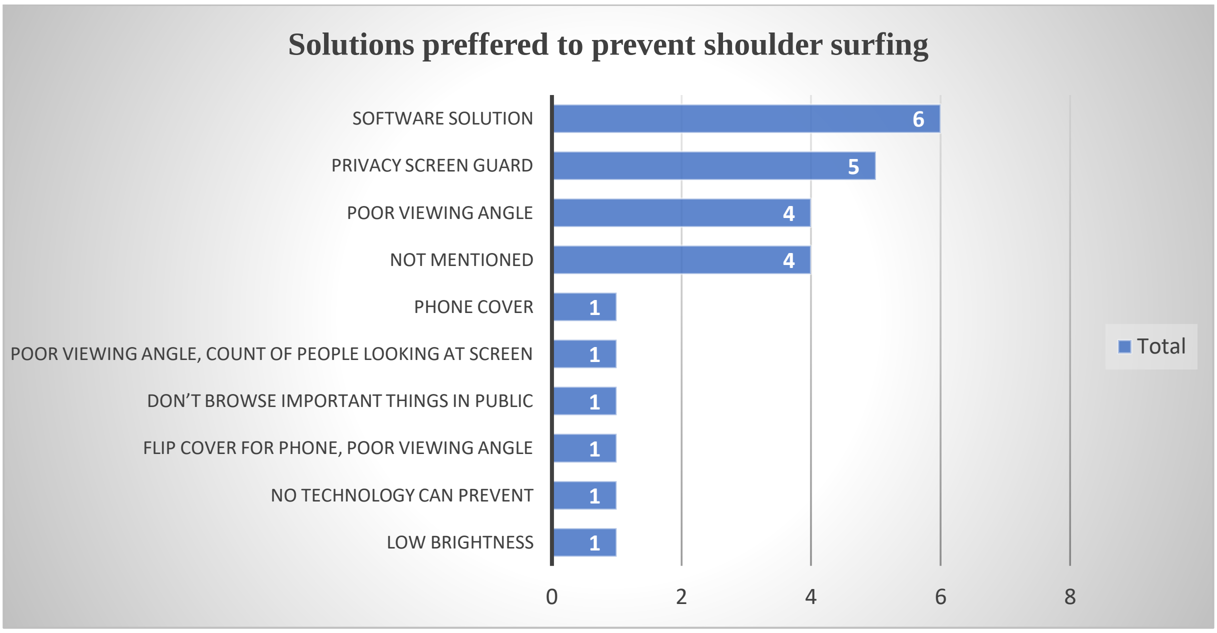


Figure 5: Graph depicting the solutions preferred by participants during shoulder surfing scenarios

4.4 Post Analysis

The hardware-based solution of privacy screen guards is one of the preferred solutions but its availability is very low considering the varied sizes and types of device screens that are available in the market, along with the additional cost that it adds for the user to invest in to protect their privacy. However, a software solution would not such a problem of being compatible with different screens as they could be embedded in the operating system and work seamlessly as a normal background application. It was also evident from the analysis that most of the participants wanted a software solution to prevent or be notified in case of a shoulder-surfing scenario. This was the motivation that was taken to move forward with the next steps of the thesis. The next step was to think of developing or enhancing a software-based solution that could help to either prevent shoulder surfing or to notify the person A of their surroundings. Eye-tracking was used and hence a proof of concept solution was developed which could be used to activate a potential privacy protection mechanism with the help of specific patterns made using eye movements. Further details about the design and implementation of the said proof of concept solution are discussed in section 5.

Section 5: Design and Implementation

5.1 Design

The result from the online survey showed a need for a software-based solution that could be used to pave a way to activate one of the privacy protection mechanisms. There were a few solutions previously proposed for iOS-based smartphones, specifically for the ones having depth-sensing cameras. On exploring and researching for solutions and libraries for android platform, very few were to be found. The choice of the android application was easy due to reasons that no solution was present prior to this in android, it occupied most of the market share until January 2019 and the fact that the author had some development experience with android. The thought-process started with studying how eye movements could be tracked with a normal front facing the camera in today's smartphones.

There was a very limited number of libraries that allow for the eye movements to be tracked and even fewer that enabled pupil tracking in the of designing. The first one was from the tech giant Google named Cloud Vision API. This library is used for understanding texts from images, emotions from faces in the pictures, track eyes blinks, and the facial gestures like a smile(Google Cloud Vision API, 2019; Google, 2019). The other library is called open-source computer vision (OpenCV). This library has many inbuilt functionalities like object detection, image processing, video analysis, graph API, deep neural networks, etc. (Open CV, 2019). Both libraries were used separately to develop sample applications that use face and eye gestures and pupil tracking. At the end after discussion with the supervisor and considering the overall aim of the thesis, the application using the OpenCV library was decided as a comparatively better solution to move forward with.

The choice to opt for the OpenCV library over Google Vision AI was primarily because of the reason that using the OpenCV library could be used up to a certain extent to track the pupil movements. On the other hand, the Google Cloud Vision API had capabilities only to detect facial gestures like smile and in terms of eye movements, only the blink of an eye could be detected. This could prove to be useful to face gesture-based applications but did not seem an ideal match for the purpose of this thesis. The other reasons included that the smile and eye blinks are a very natural behavior and hence would have triggered the actions embedded in the application and hence would have been error prone. This was realized upon implementing and testing the application on an android phone.

5.2 Implementation

5.2.1 Google Cloud Vision API Based Application

The implementation of the android application using Google Cloud Vision API was done at first and aimed at playing or pausing video only when the user of the phone would have had both eyes open and smiling. If either one of the above criteria would have not been met, the video playback would have been paused and would have displayed a proper message on the screen for the user to take further action on. A minimum threshold value of 0.80 was used to detect the probability of a smile and open eyes as seen in figure 6. If the probability was lower than the threshold, then it would have been considered as closed eyes or no smile. A high threshold was chosen to eradicate the natural facial gestures of open eyes and smile.

```
// minimum threshold value to detect open eyes and smile
private final float THRESHOLD = 0.80f;
```

Figure 6: Threshold value used for detecting the probability of open eyes and a smile

Figure 7 shows the simple implementation algorithm used to detect open eyes and the smile with a probability of more than the defined threshold.

```
// check for both open eyes and smile
if ((face.getIsLeftEyeOpenProbability() > THRESHOLD || face.getIsRightEyeOpenProbability() > THRESHOLD) && face.getIsSmilingProbability() > THRESHOLD) {...}
// check for both open eyes and no smile
else if ((face.getIsLeftEyeOpenProbability() > THRESHOLD || face.getIsRightEyeOpenProbability() > THRESHOLD) && face.getIsSmilingProbability() < THRESHOLD) {...}
// for all other conditions
else {...}
```

Figure 7: Algorithm used to detect open eyes and smile using Google Cloud Vision API

The screenshots and the GitHub link for the application code of this application can be found in Google Cloud Vision API App subdirectory of code directory and in GitHub Link.txt respectively. As stated in section 5.1 this application was not further explored as it did not meet the purpose of the thesis and a pupil tracking-based approach was adopted using OpenCV which is discussed in section 5.2.2.

5.2.2 OpenCV Based Application

OpenCV is a library that has many built-in features, among which face detection and tracking is one of them. This library also includes the capability of pupil tracking using a HAAR-feature based cascade classifier to classify objects in videos and pictures (OpenCV Haar Classifier, 2018). This machine learning classifier has been used by this OpenCV library to detect eye and pupils. An initial project was implemented with a similar idea but was only limited to the detecting of the pupil of the eye using the same library but with a very old version and the development was stopped about four or 5 years back (Hosek, 2015). The base for the eye-tracking application has been motivated by the same repository and the related tutorial (Hosek, 2013) was read through for help. Since the tutorial was almost 6 years old, it was not very useful to follow the steps given in the tutorial as it used out-dated Android API levels, as well as the version of open cv that it used, had become very old. The open cv version used was 2.4.2 (Hosek, 2013) while the latest available version is 4.1.1 (OpenCV Landing Page, 2019). The version used for the application developed in this thesis is 3.4.3 as the compatibility of this version with android is good. The Android API level used for this application is level 28, otherwise called as android pie.

The first step in working on the application is the detection of the face using the front camera of the smartphone. After its detection, the different landmarks of the face are detected, for example, eyes, ears, mouth, forehead, nose, etc. All the landmarks which are not required in this application are ignored and removed and then only the eye area is calculated. The detection of the face is shown by a red color box. The next step is to reduce the face features to eyes only. This is done by using simple mathematical calculation and assumption keeping some margin of error as the eye box does not only cover the eyes but some area of the face in it too. Once that it has done, the classifier is then applied to both the eyes that detect the pupils of the eye and then learns for initial frames as a training set.

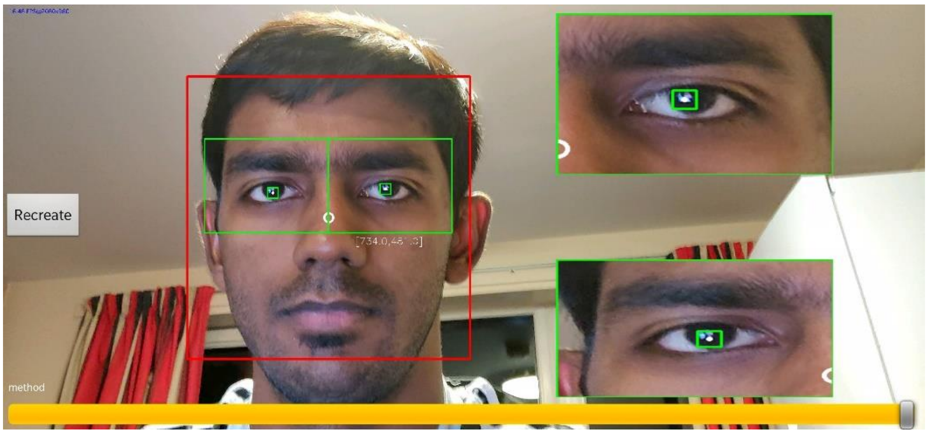


Figure 8: Learning phase in the android application

A scale factor of 1.05 for the classificator detectMultiScale is used in the code for this learning phase, which performs the best (obtained using multiple testing done by the author during development). During the learning phase, the application detects the eye pupils as a green box (see figure 8) and then turns into a yellow box when the actual tracking starts. To help users understand how this works, the direction in which each of the eyes is looking at is displayed on the screen.

The application works in a manner that it learns for the first 100 frames and then matches the eyes with the defined classifier and tracks it. A lot of methods previously used in the library had become outdated and did not exist now. They all had to be replaced in 3.4.3 with the newer ones available for example, class Core is now deprecated and replaced by Imgproc class. The application gives the user several options for template matching like TM_SQDIFF, TM_SQDIFF_NORMED, TM_CCOEFF_NORMED, etc. These methods use predefined template matching formulas which can be seen in (Open Source Computer Vision, 2019).

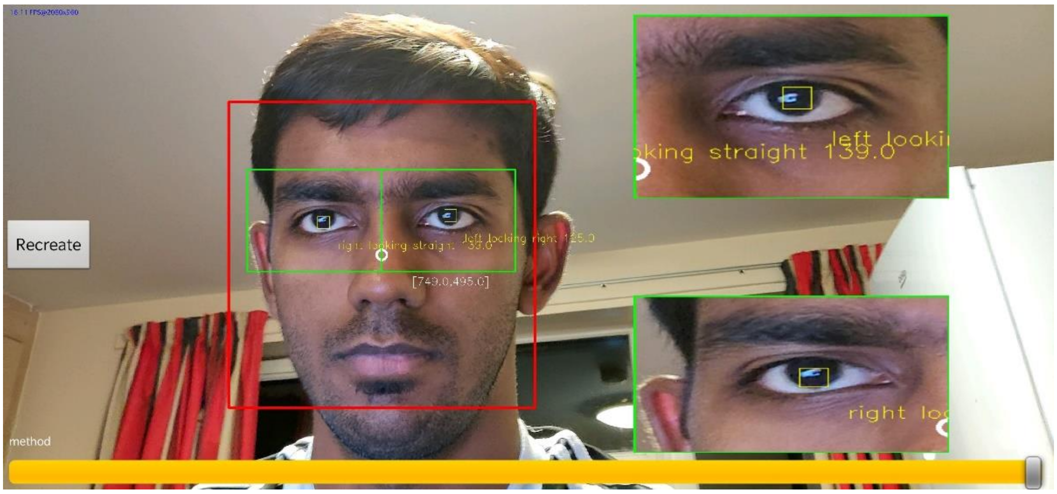


Figure 9: Normal method user looking straight

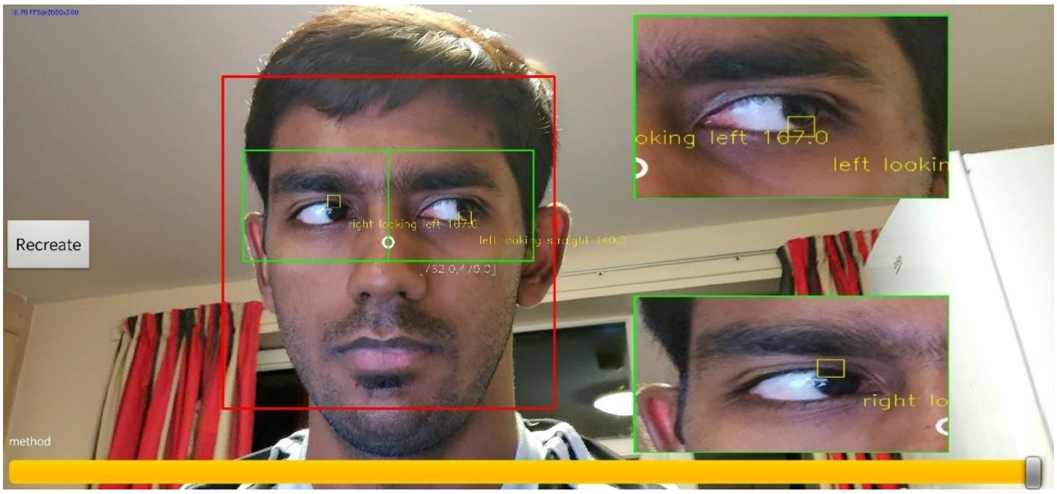


Figure 10: Normal method user looking left

From testing the application, it was understood that the method named TM_CCOEFF_NORMED gave the best results and this is in line with the results of testing done in (Open Source Computer Vision, 2019). The screenshots of the application can be found in figure 8 to 13. From the screenshots of the application when the user is looking straight, the right eye displays the correct information while the information for the left eye is incorrect (see figure 9).

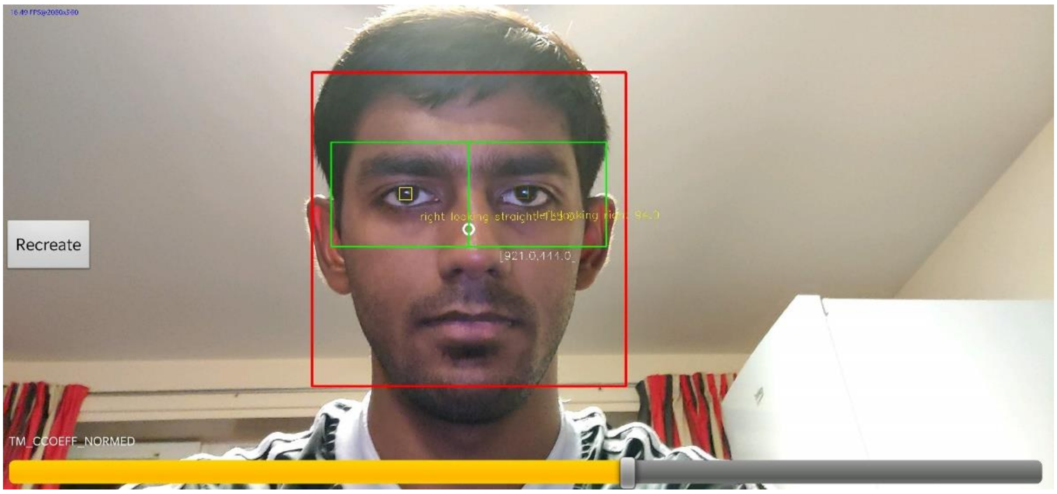


Figure 11: TM_CCOEFF_NORMED method and user looking straight

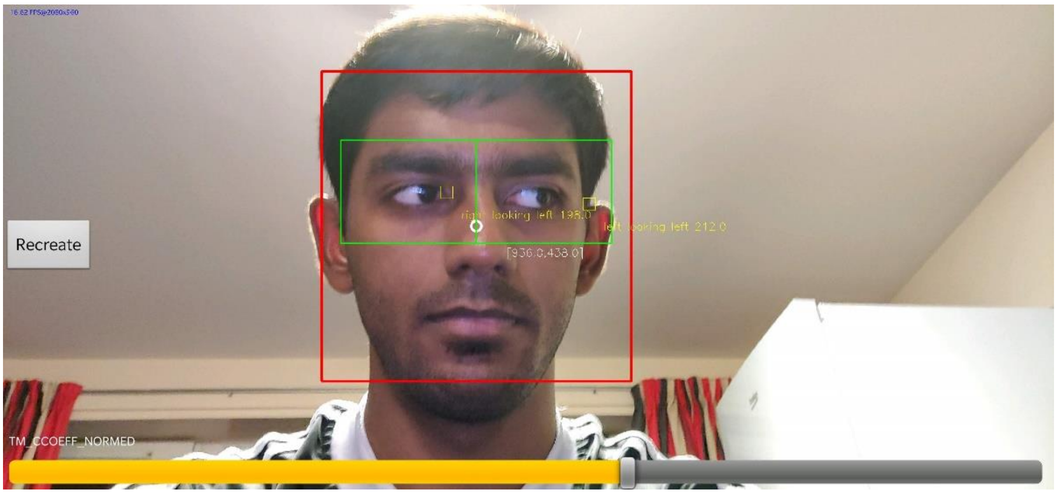


Figure 12: TM_CCOEFF_NORMED method and user looking left

The same happens for when the user looks right or left and the tracker for left eye pupil misbehaves. The problem is partially rectified if the template matching pattern is changed to TM_CCOEFF_NORMED which is evident from the screenshots (figure 11 to 13). The problem of incorrect direction being shown when the user looking straight for left eye persists (figure 11), but it displays the correct information for when the user looks left or right even though the tracker is misplaced slightly (see figure 12 and 13).

The GitHub code for the above application can be found in GitHub_Link.txt file under OpenCV Android App directory of code.

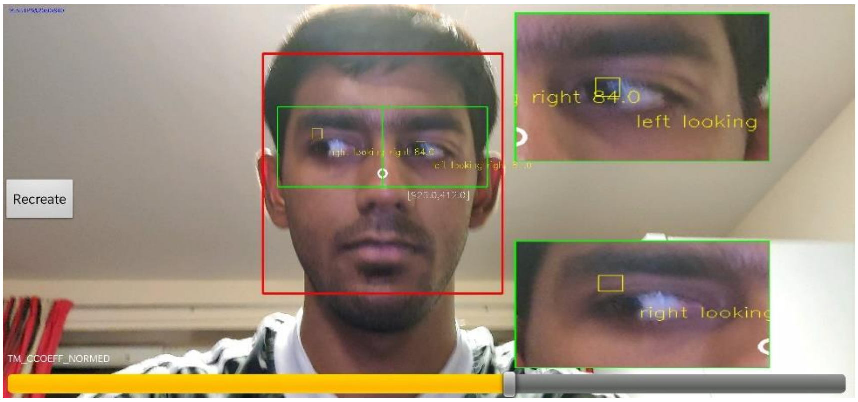


Figure 13: TM_CCOEFF_NORMED method and user looking right

The application also provides a recreate button on the left middle side of the screen that can be used to reset all the previous learnings of a matching method. This is helpful in scenarios where the user wants to change the template matching algorithm. The calculation of if the user is looking left, right or straight was done based on the difference of the distance calculated between yellow box and then green box boundary (the left boundary of the green box when calculating left gaze direction and the right boundary for right gaze). The motivation of calculating the direction using the distance between the yellow and green box was taken from Zhang et al. The code screenshot in figure 14 depicts the simple algorithm used to calculate the direction in which user is looking. The ranges are decided based on several trial runs done by the author himself on multiple scenarios during the development phase.

```
if ((matchLoc_tx.x-area.tl().x) < 130) {
    Log.i(eyeType, msg: eyeType + " looking right");
    Imgproc.putText(mRgba, text: eyeType + " looking right " + (matchLoc_tx.x-area.tl().x),
            new Point( x: matchLoc_tx.x + 40, y: matchLoc_ty.y + 40),
            Core.FONT_HERSHEY_SIMPLEX, fontScale: 0.7, new Scalar(255, 255, 0,
                    255));
} else if ((matchLoc_tx.x-area.tl().x) > 160){
    Log.i(eyeType, msg: eyeType + " looking left");
    Imgproc.putText(mRgba, text: eyeType + " looking left " + (matchLoc_tx.x-area.tl().x),
            new Point( x: matchLoc_tx.x + 40, y: matchLoc_ty.y + 40),
            Core.FONT_HERSHEY_SIMPLEX, fontScale: 0.7, new Scalar(255, 255, 0,
                    255));
} else if ((matchLoc_tx.x-area.tl().x) > 130 && ((matchLoc_tx.x-area.tl().x) < 160)){
    Log.i(eyeType, msg: eyeType + " looking straight");
    Imgproc.putText(mRgba, text: eyeType + " looking straight " + (matchLoc_tx.x-area.tl().x),
            new Point( x: matchLoc_tx.x + 40, y: matchLoc_ty.y + 40),
            Core.FONT_HERSHEY_SIMPLEX, fontScale: 0.7, new Scalar(255, 255, 0,
                    255));
} else {
    Log.i(eyeType,  msg: eyeType + " looking random place");
    Imgproc.putText(mRgba, text: eyeType + " looking random place " + (matchLoc_tx.x-area.tl().x),
            new Point( x: matchLoc_tx.x + 40, y: matchLoc_ty.y + 40),
            Core.FONT_HERSHEY_SIMPLEX, fontScale: 0.7, new Scalar(255, 255, 0,
                    255));
}
```

Figure 14: Sample code to show the calculation of direction in which the user is looking at one point of time

Section 6: Testing and Evaluation

6.1 Testing

The testing phase was carried out with 15 participants which were aimed at two prime things. The first thing in focus was to understand in depth about how relationships impact the suitability of the privacy protection and notification mechanisms for any user in day to day life, mainly in cases of shoulder surfing. Some of the mechanisms are dimming filter mask, crystallize filter, fake text, vibrating alert, low brightness, etc. (Khamis, Eiband, et al., 2018; Zhou et al., 2015; Saad et al., 2018; ACM SIGCHI, 2016). To proceed ahead with the testing phase, short videos of 13 to 14 seconds were made where the main idea was that person B tries to observe the contents of person A and then on realizing that B is shoulder surfing, A tries to make a pattern with the eyes using the full-fledged working application version of the proof of concept application developed in this thesis to activate one of the privacy protection mechanisms. The other scenario in this video is when the phone using its own background process and possibly using the better version of same application detects the attackers and instead of activating any privacy protection mechanism, it notifies person A in one way or the other about the possibility of them being shoulder surfed at that moment.

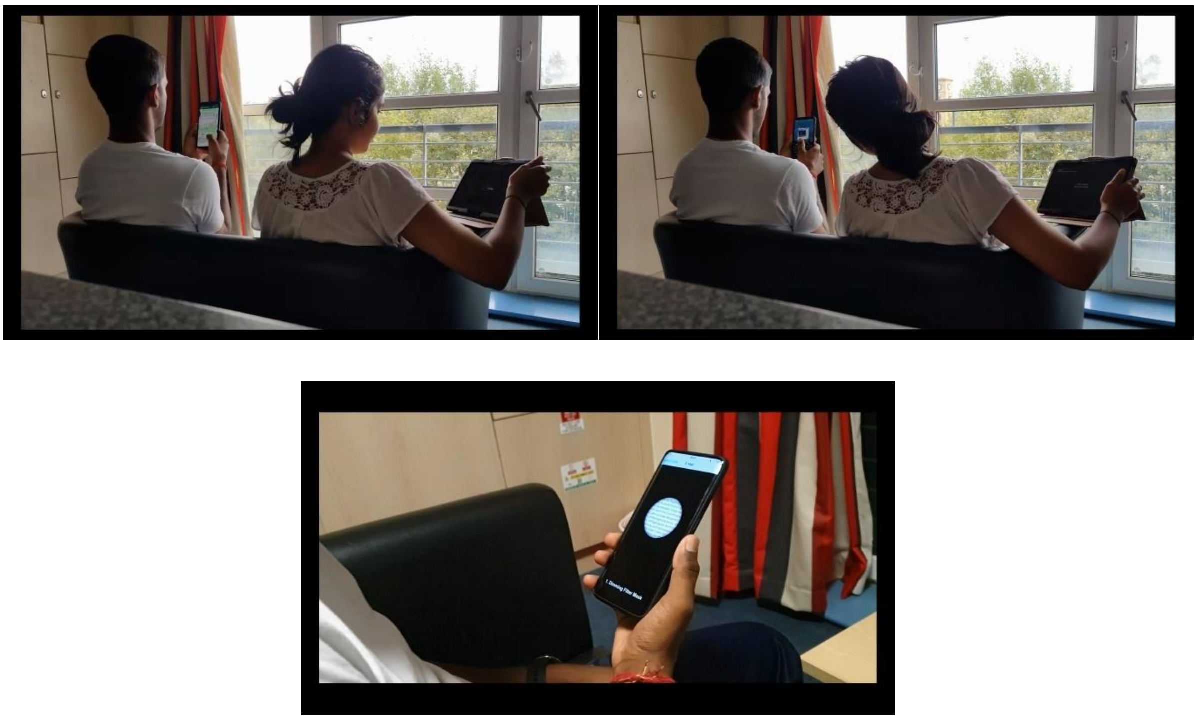


Figure 15: Screenshots of the prototype application during the testing phase. From Left to right to below them, the first picture shows 2 people using their smartphones when person B decides to attach person A and then the third picture shows how the phone will cope-up with protection of the eyes.

The mechanisms were hence classified into two groups, one being privacy protection mechanism (hence-forth referred to as category 1) while the other being privacy protection notification mechanism (hence-forth referred to as category 2). The category 1 included dimming filter mask, crystallize filter, fake text, no filter, grayscale, low brightness, selective hiding, and selective showing while category 2 included notification via front flash (if available in the smartphone), front camera preview, vibrating alert, and an alert icon of some sort appearing on the screen. Using both categories, 12 different short videos were made which were shown to the participants one by one.

To understand the impact of relationships on the suitability of these mechanisms, a questionnaire was prepared which consisted of 10 questions, out of which 8 were relationship dependent questions, while one questions were related to participants' input of the most suitable mechanism. The last question was an open-ended feedback question where at the end of the study each participant was shown the working of the android application implemented in this thesis and then their collective feedback was noted regarding the application.

After watching each video, the participants were asked to answer questions numbered from 1 to 8 and at last questions 9 and 10. For each of question 1 to 8, they were given the 12 options of category 1 and 2 combined in a definitive order which they were asked to rate on a scale of 1 to 5 based on the suitability of the relationship mentioned in that question. 1 was the least suitable mechanism and 5 was considered as the most suitable mechanism for that relationship. At the end of the survey, that is after answering all the questions, each participant was asked for reasons about them giving high scores to one or more mechanism for each relationship and their thought process in doing so. The detailed instructions for the participants could be found in the Evaluation study questionnaire subdirectory and the question format could be referred from the same document. The different results and inferences in discussed in section 6.2.

6.2 Evaluation of Test Results

The results of the testing data in excel tables represented as image captures can be found in Evaluation study responses subdirectory of the code directory.

6.2.1 Quantitative Discussion

After collecting all the responses from 15 participants, all the data was formatted onto an excel workbook with each sheet depicting each question response. All the responses could be accessed via https://bit.ly/2kfXutR. On roughly analyzing the responses for each relationship for different mechanisms, it shows that participants' choice of protection or notification mechanism is highly dependant on the type of relationship they have with the person B.

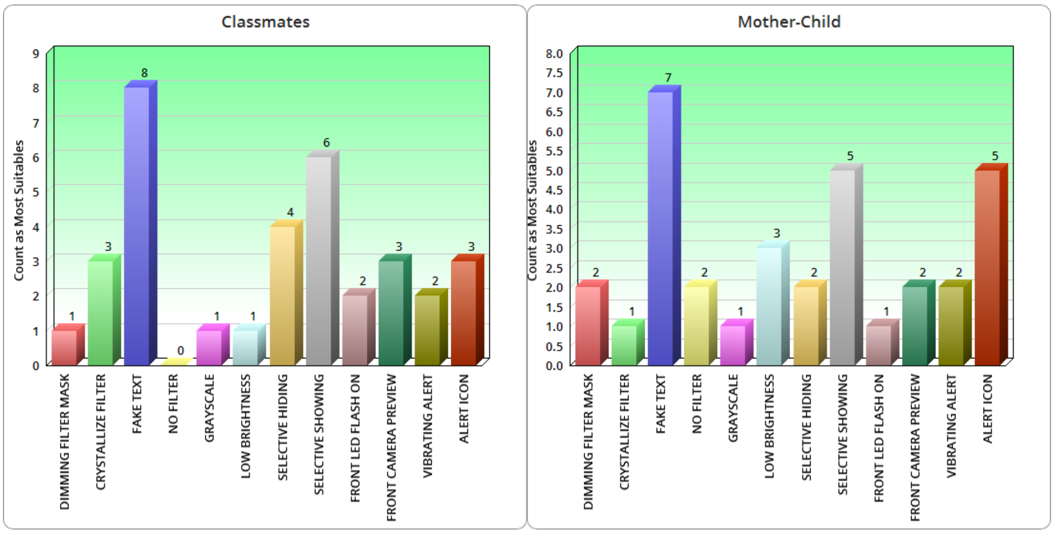


Figure 16: (LEFT) Graph displaying the suitability of different mechanisms for Classmates, (RIGHT) Graph displaying the suitability of different mechanisms for Mother-Child

Analyzing the responses from the testing phase, the result clearly indicates a big impact of change in the relationships on the suitability of the privacy protection and notification mechanisms. The different relationships considered during the testing study were those of classmates, mother-child, father-child, friends, strangers, siblings, a professional relationship and with that of partners. The most suitable mechanism for classmates as the relationship was fake text (see figure 15 – left).

The responses received for the most suitable mechanism for mother-child and father-child relation were very similar in nature. Both relationships saw the suitability of fake text as being the highest while the next one opted were selective showing as alert icons to notify the users of their environment (see figure 15 – right and figure 16 – left).

When participants were asked about their choice of the mechanism when around with friends (see figure 16 – right) or siblings (see figure 17 – right), the most common response was that of fake text and selective showing.

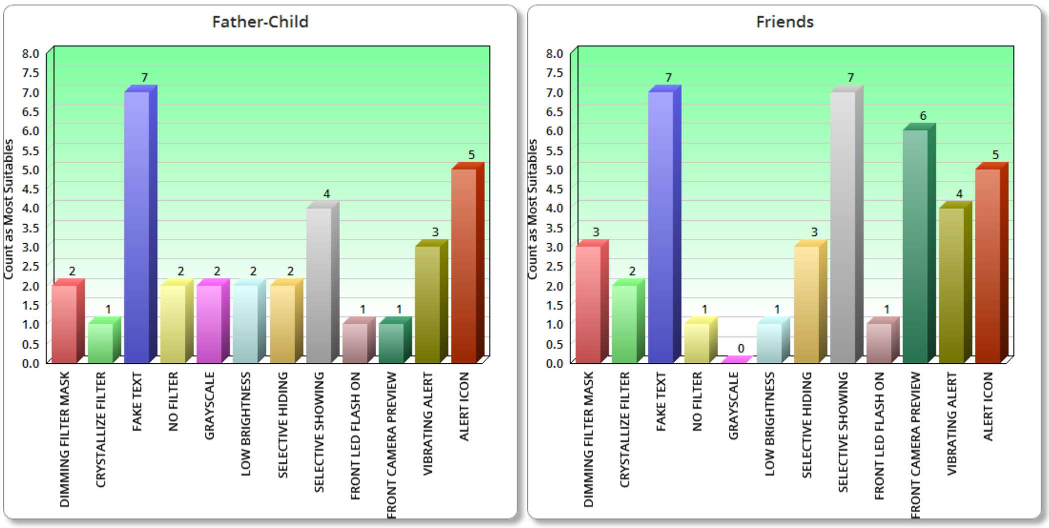


Figure 17: (LEFT) Graph displaying the suitability of different mechanisms for Father-Child, (RIGHT) Friends

However, participants also opted for being notified by the means of the front camera preview, vibrating alert or with an alert icon on their screen if their friends were to shoulder surf them.

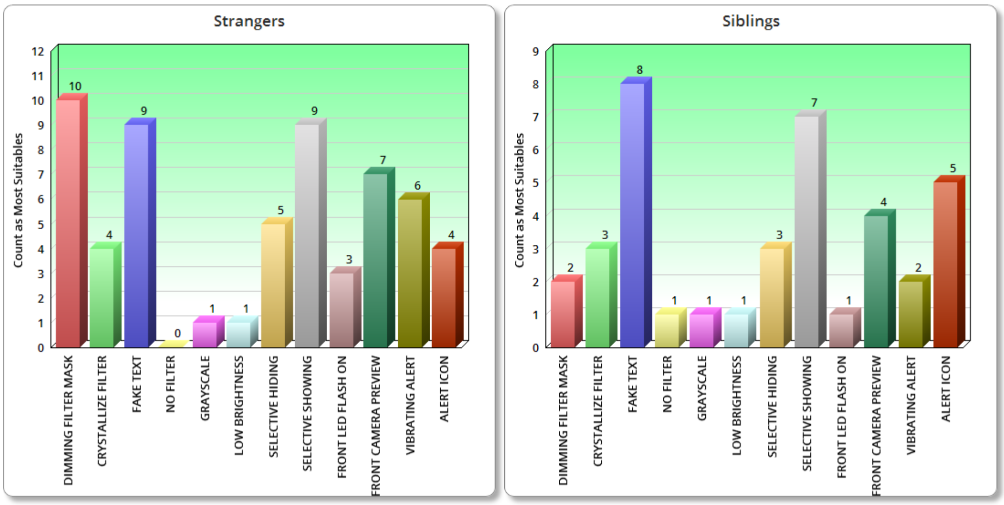


Figure 18: (LEFT) Graph displaying the suitability of different mechanisms for Strangers and (RIGHT) Siblings

When around strangers, no one preferred a no filter mechanism which enables the attacker to observe all their phone's content and most of the participants wanted a way to hide their content using of way or the other. The most suitable mechanisms were dimming filter mask, fake text, and selective showing for strangers (see figure 17 – left).

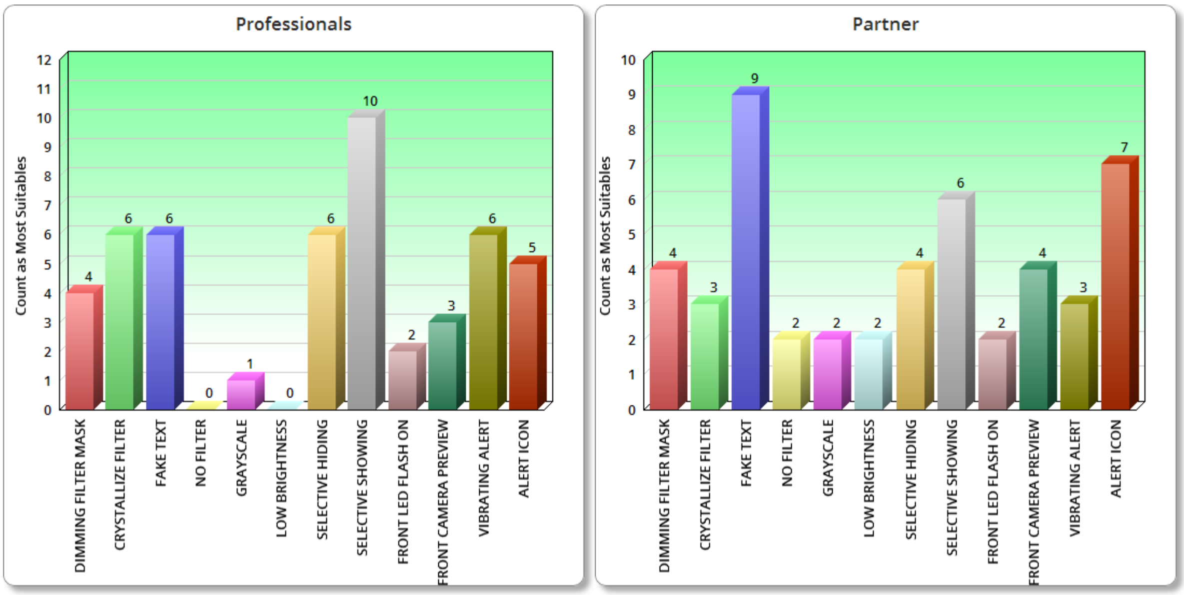


Figure 19: (LEFT) Graph displaying the suitability of different mechanisms for Professionals, (RIGHT) Graph displaying the suitability of different mechanisms for Partner

While the fake text was considered as the most suitable privacy protection mechanism when participants were around their partners (see figure 18 – right), it was considered as one of the second go-to options when they were around professionals (see figure 18 – left). The most suitable mechanism for participants in office environments was for their smartphones to switch to a selective showing mechanism.

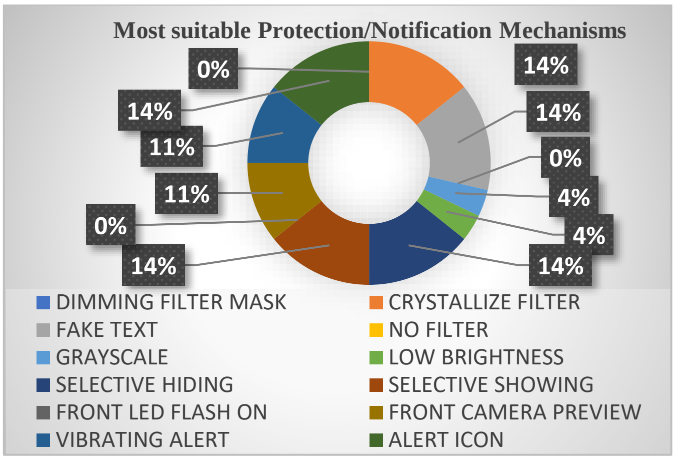


Figure 20: Graph depicting the most suitable privacy protection or notification mechanism overall

When participants were asked to choose the most suitable privacy protection or notification mechanism, the most suitable mechanisms were crystallized filter, fake text, selective hiding, selective showing, or getting notified using an alert icon with each of them getting 4 responses (14% votes each – see figure 19). No participant chose the dimming mask filter, no filter or front camera led flash as their scores remained at zero.

6.2.2 Qualitative Discussion

Participants were also asked for a reason for them choosing one or more most suitable mechanisms for every relationship question (1 to 8). With people that are known, close to or related to (such as mother, father, sibling or partner), the majority of the participants, while opting for a protection mechanism, factor in the idea that the relationship with such people not be affected in a negative way. The feelings usually avoided in such cases is that of being embarrassed, or awkward. On the other hand, as some of these relationships occupy a position of authority, the attempt is to be more subtle in the act of protecting the contents of their device.

In the case with strangers, people are more conscious about protecting the contents of their device and have mostly opted for the protection mechanisms over notification mechanisms such as alert icon, low brightness, grayscale, etc. Most of the participants have as a result selected a protection mechanism that hides or distorts part of the text which would make it difficult for the shoulder surfer to understand the context of the information being accessed by the user. In addition to this, all participants believe that some sort of mechanism is required to protect their data in the presence of strangers as none of the participants opted for "no filter". This is in opposition to a few other relationships such as parents or siblings wherein some participants felt that no protection mechanisms are required. In addition to this, while the participants actively attempted to avoid impacting the previous relationship negatively, in the case of strangers, participants often didn't mind openly indicating or in some cases even telling the shoulder surfer to stop breaching their privacy by means of these mechanisms.

In relationships such as classmates and professionals, (the latter including work colleagues etc) as the degree of familiarity and trust can vary with each individual the participants display an assortment of opinions on the type of protection mechanism that is the most adequate, while agreeing that some type of mechanism is required as the "no filter" option was not considered suitable by any participant.

Based on the current version of the application, most participants felt that, given the fact that the app would require the phone camera to be in constant use tracking the eye movement, it would strain the phone battery. This could cause problems while traveling as the phone battery would not last long and as a result, the app would only be compatible with phones having a large battery backup and high-quality wide lens camera. The scope of application for the app would, therefore, be greatly reduced. One of the suggestions provided to counter this was installing a feature to switch the app on or off at will.

Apart from this, the participants also pointed out that the app might face difficulties in detecting the eyes if the face is out of range or if the user is wearing glasses or shades. They also suggested that it would be more helpful if the phone could detect the shoulder surfer on its own, instead of the user having to be aware of shoulder surfers as most of the times the user might be too engrossed in his work to be as aware of his/her surroundings. Concerning the mechanisms discussed within this report, especially the "notification mechanisms", the participants felt that they would be less than useful when incorporated within the app as they would do nothing to "protect" the data of the user. However, their utility would increase if, as suggested above, the app detected the shoulder surfer on its own and then uses these mechanisms to notify the user.

On the other hand, while the protection mechanisms discussed within the report might be very useful in public places and offices, many of the participants were unsure of their utility at home as often close relationships people often assume a position of authority and ask questions. A suggestion that was tailored to such a situation, with members of the family, was a mechanism that would switch screens and would be based on alert mechanisms.

Section 7: Conclusion

7.1 Current Issues

The thesis covered for many issues while exploring a new area of dependency of relationships on responses of shoulder surfing. The study conducted, both the initial survey, as well as the final testing and evaluation study, is conducted for 25 and 15 participants respectively. The thorough study done is not enough to generalize the results from the survey and hence it would prove to be very interesting to collect data from a larger number of participants. The implementation of the prototype application using open cv library received constructive feedback during evaluation. The prime issue of the working of the application would be the two things. Firstly, the accuracy with which the application correctly detects the gaze direction of the user and secondly how seamless would its integration with android operating system prove to be considering its high battery consumption as it would need to use the front camera at all times in the background whenever its related feature would be turned on. This was also a common concern the participants expressed in the evaluation of the application. Finally, a limitation for the various privacy protection mechanism discussed in this thesis is that they would work fine for only textual documents and related applications but not for photos and videos as the user would not want part of the photos or videos being hidden while they access them, independent of the relationship and the environment of use. Most of the responses received in both the online survey and the evaluation study are from South Asians, thus cannot be generalized to other countries by default, but it does prove to be a good start to understand the impact of the relationship on responses to shoulder surfing.

7.2 Future Work

The working of the prototype android application could be enhanced and combined with the face recognition technology which works perfectly in available smartphones. This would enable the application to distinguish the owner face from the other faces available in its view. This would also reduce its background work of tracking only the pupils of the registered face and if that is not found in the camera view, then no further processing would be performed, thus reducing the battery to an extent. By implementing the application in such a way, it could be made possible to count the different number of faces available around the user of the smartphone as this was one of the requested features from the participants in the initial online survey. More data is needed to generalize the impact of the relationship on response to shoulder surfing scenarios that would prove helpful in deciding the most suited course of action for different relationships. Once the eye tracking is done, a number of eye patterns could be registered in the phone that would then be used to activate some of the privacy protection mechanisms that is best suited for different relationships.

7.3 Summary

This thesis focused primarily on how people's reactions and feelings change to shoulder surfing scenarios if the relationship between person A and B changes, where they could be acting as either of them. Initial data were collected for analyzing this impact, to gather the requirements and the most requested feature from the participants. Hardware and software solutions were the most preferred ones among others. Based on the most commonly requested feature, a prototype application was developed to track the eye movements to detect the direction in which the user of the smartphone was looking in. This application was then used as a possible means to activate different privacy protection mechanisms to protect person A from getting their contents being observed without their consent. Open-ended feedback was then taken from the participants about the application enhancements and possible issues along with their preference of privacy protection and notification mechanisms in terms of suitability. It is concluded from the thesis study that relationships play a vital role not only in how people respond to shoulder surfing scenarios but also how they want their privacy to be protected from others.

Bibliography

ACM SIGCHI (2016) *Enhancing Mobile Content Privacy with Proxemics Aware Notifications and Protection*. Available from: <https://www.youtube.com/watch?v=Q_hVu7-9kC4> [Accessed 22 August 2019].

Casserly, M. (2019) Which is the more popular platform: iPhone or Android? [Internet]. Available from: <https://www.macworld.co.uk/feature/iphone/iphone-vs-android-market-share-3691861/> [Accessed 30 August 2019].

Eiband, M., Khamis, M., von Zezschwitz, E., Hussmann, H. & Alt, F. (2017) Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. Denver, Colorado, USA, ACM Press, pp.4254–4265. Available from: <http://dl.acm.org/citation.cfm?doid=3025453.3025636> [Accessed 25 August 2019].

Flast, B. (2014) *Android Eye Tracking prototype for team theia*. Available from: <https://github.com/baf509/Android_Eye_Tracker> [Accessed 25 August 2019].

Google (2019) Vision AI | Derive Image Insights via ML [Internet]. Available from: <https://cloud.google.com/vision/> [Accessed 2 September 2019].

Google Cloud Vision API (2019) Cloud Vision API | Cloud Vision API Documentation [Internet]. Available from: <https://cloud.google.com/vision/docs/face-tutorial> [Accessed 2 September 2019].

horstlb (2015) *This is an Eye-Tracking Android Studio Project which captures Eye-Gestures to unlock the Smartphone Screen.: horstlb/EyeTrackingLockScreen*. Available from: <https://github.com/horstlb/EyeTrackingLockScreen> [Accessed 25 August 2019].

Hosek, R. (2013) Android eye detection and tracking with OpenCV. *Android eye detection and tracking with OpenCV*. Available from: <http://romanhosek.cz/android-eye-detection-and-tracking-with-opencv/> [Accessed 25 August 2019].

Hosek, R. (2015) *Simple sample for eye tracking with OpenCV*. Available from: <https://github.com/hosek/eyeTrackSample> [Accessed 25 August 2019].

Khamis, M., Alt, F. & Bulling, A. (2018) The past, present, and future of gaze-enabled handheld mobile devices: survey and lessons learned. In: *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '18*. Barcelona, Spain, ACM Press, pp.1–17. Available from: <http://dl.acm.org/citation.cfm?doid=3229434.3229452> [Accessed 25 August 2019].

Khamis, M., Eiband, M., Zürn, M. & Hussmann, H. (2018) EyeSpot: Leveraging Gaze to Protect Private Text Content on Mobile Devices from Shoulder Surfing. *Multimodal Technologies and Interaction*, 2 (3), p.45.

Lamé, A. (2019) *👀 Eye Tracking library easily implementable to your projects: antoinelame/GazeTracking*. Available from: <https://github.com/antoinelame/GazeTracking> [Accessed 30 August 2019].

Majaranta, P. & Bulling, A. (2014) Eye Tracking, and Eye-Based Human-Computer Interaction. In: S. H. Fairclough & K. Gilleade eds. *Advances in Physiological Computing*. London, Springer London, pp.39–65. Available from: <http://link.springer.com/10.1007/978-1-4471-6392-3_3> [Accessed 25 August 2019].

Marques, D., Guerreiro, T., Carriço, L., Beschastnikh, I. & Beznosov, K. (2019) Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. Glasgow, Scotland Uk, ACM Press, pp.1–13. Available from: <http://dl.acm.org/citation.cfm?doid=3290605.3300819> [Accessed 25 August 2019].

Matheus, A. (2017) Eye Tracking for Mouse Control in OpenCV - Tango with code [Internet]. Available from: <https://picoledelimao.github.io/blog/2017/01/28/eyeball-tracking-for-mouse-control-in-opencv/> [Accessed 30 August 2019].

Open CV (2019) OpenCV: OpenCV Tutorials [Internet]. Available from: <https://docs.opencv.org/master/d9/df8/tutorial_root.html> [Accessed 2 September 2019].

Open Source Computer Vision (2019) OpenCV: Template Matching [Internet]. Available from: <https://docs.opencv.org/3.4/de/da9/tutorial_template_matching.html> [Accessed 25 August 2019].

OpenCV Haar Classifier (2018) OpenCV: Face Detection using Haar Cascades [Internet]. Available from: <https://docs.opencv.org/3.4.1/d7/d8b/tutorial_py_face_detection.html> [Accessed 2 September 2019].

OpenCV Landing Page (2019) OpenCV [Internet]. Available from: <https://opencv.org/> [Accessed 2 September 2019].

Saad, A., Chukwu, M. & Schneegass, S. (2018) Communicating Shoulder Surfing Attacks to Users. In: *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia - MUM 2018*. Cairo, Egypt, ACM Press, pp.147–152. Available from: <http://dl.acm.org/citation.cfm?doid=3282894.3282919> [Accessed 22 August 2019].

Zhang, Y., Bulling, A. & Gellersen, H. (2013) SideWays: a gaze interface for spontaneous interaction with situated displays. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*. Paris, France, ACM Press, p.851. Available from: <http://dl.acm.org/citation.cfm?doid=2470654.2470775> [Accessed 25 August 2019].

Zhou, H., Ferreira, V., Alves, T., Hawkey, K. & Reilly, D. (2015) Somebody Is Peeking!: A Proximity and Privacy Aware Tablet Interface. In: *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '15*. Seoul, Republic of Korea, ACM Press, pp.1971–1976. Available from: <http://dl.acm.org/citation.cfm?doid=2702613.2732726> [Accessed 22 August 2019].