Design of a smartphone application that provides user generated emergency warnings for fire incidents

A thesis presented for the degree of
Master of Science

Supervisor:

Prof. Daniela Carrion

Written by:

Florenc Bosi

(919433)

Civil Engineering for Risk Mitigation

School of Civil, Environmental and Land Management Engineering

Politecnico di Milano

Lecco

December 2021

Sommario

Con il passare degli anni, possiamo vedere che il progresso tecnologico quando si tratta di comunicazione è stato enorme, siamo passati dal parlare tra di noi su un telefono fisso alla possibilità di fare videochiamate con tutte le persone che vogliamo contemporaneamente in qualsiasi momento e ovunque vogliamo; la comunicazione è diventata più immediata per il fatto che ognuno ha uno smartphone in suo possesso, è un’estensione della nostra mano. Il problema, però, sta nel fatto che la comunicazione, sebbene sia immediata, è anche si può comunicare solo con le persone di cui si dispone dei dati personali, che siano il loro numero di telefono, il loro nome utente del social network o la loro e-mail, il che significa che la comunicazione è davvero immediata ma anche limitata alla cerchia di ognuno. Questo vale per le comunicazioni quotidiane con le persone che si hanno all’interno della propria cerchia, ma cosa succede in caso di emergenza? Come si potrebbe rompere quella barriera di questa comunicazione limitata in caso di emergenza? Questa tesi discute esattamente questo, presenta il design di un’applicazione che potrebbe rompere quella barriera, un’applicazione che dà il potere all’utente di avvertire gli altri essere umani anche se non li conosce affatto, semplicemente inviando avvisi di emergenza. Più specificamente, questa tesi elabora avvisi di emergenza generati da altri utenti durante incidenti relativi a incendi.

Parole Chiave – smartphone, comunicazione, avvisi di emergenza, incendi

Abstract

As the years pass, we can see that the technological progress when it comes to communication has been huge, we went from being talking with one another over a fixed phone to being able to have video calls with as many people as we want at the same time anytime and anywhere we want; communication has become more immediate due to the fact that everyone has a smartphone on their possession, it is an extension of our hand. The issue though, lies with the fact that although the communication is immediate, it is also limited. You can communicate only with the people that you have personal information about, whether that is their phone number, their social network username or their e-mail, meaning that communication is indeed immediate but also limited to one’s circle. This applies to everyday communications that people have within their own circle, what happens though in case of emergencies, how could one break that barrier of this limited communication in case of an emergency? This thesis discusses exactly that, it presents the design of an application that could break that barrier, an application that gives the power to the user to warn other people even if he does not know them at all simply by sending emergency warnings. More specifically, this thesis elaborates emergency warnings during fire related incidents that are generated by other users.

Keywords – smartphone, communication, emergency warnings, fires

Dedication

To my parents, thank you for always believing in me and supporting me throughout this journey.

To all the new friends I made, in happiness and sorrows, thank you for always being there.

Acknowledgements

Thank you to my supervisor, Prof. Daniela Carrion, for your patience, guidance, and support. I am extremely grateful that you took me on as a student, but most importantly, thank you for taking a chance on me and worked on something that relatively speaking was outside of the field of your expertise.

I would like to also thank my parents, my two sisters and my friends. I am grateful for your unconditional, unequivocal, and loving support, continuous encouragement and hope that you gave me. Without any of these, this thesis would not have been possible. Thank you all for the strength you gave me. I love you all!

Contents

1. Introduction

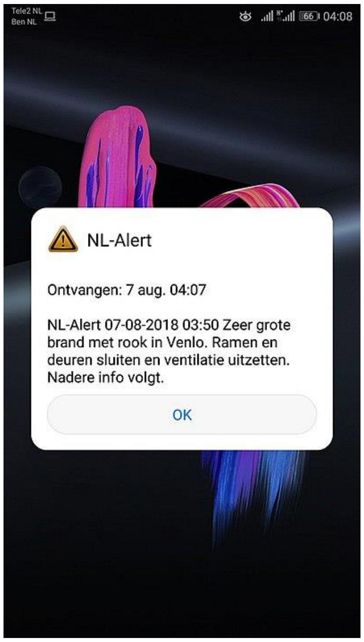
During July of 2018, on the Attica wildfires in Greece, 103 people died and more than 140 were injured, many of which with severe burns. It was the second deadliest wildfire related incident of the 21st century. Among the victims there were kids, elderly, men and women; entire families died that day. The Attica wildfires are not the topic of this thesis and thus we should focus on a specific incident that occurred on the 23rd July 2018. To be more precise, there was a group of 26 people which had not realized that the fire had broken out earlier until it was close to them, by the time they found out about it, it was already too late, they ran for their lives but with no avail, as a result they ended up on the backyard of a house trapped from all the sides by the wildfire while also having a cliff behind them. Those 26 people died that day. This incident begs the question, what if they had known earlier about the fires, what if they were warned about the fires before it was too late, how many of those 26 people could have been saved? We do not know and most likely we will never know how things could have been if these people had been warned about the incident, what we can learn from it though, is that if people are warned for such incidents ahead of time, even by a few minutes, many lives could be saved in the future. This brings us to the purpose of this thesis, the topic is the design of an application that would provide user generated emergency warnings for fire incidents, something that I firmly believe that if it existed during those wildfires of 2018, many of those 26 people would be alive today. This thesis examines the concept of the existence of such application in today's world, what would be needed for it to be realized, the background of the application as well as the process and method that it would function and operate in the instance of a fire incident.

2. Applications and existing technologies that provide emergency warnings to the public

The idea of using emergency alerts that are location based and broadcasted to cellular devices is not a new one. During the past years, there have been several examples of applications for Wireless Emergency Alerts (WEA) or Cell Broadcasting, have been utilized in order to provide security to the public across several countries in the world. The main target of those alert systems is analogous to the one that is presented in this thesis, the rapid alert of a specific group of people that is at risk from a catastrophe or extreme natural phenomena, the evacuation of that specific area and seek of shelter or protection.

2.1 NL-Alert System (the Netherlands)

The NL-Alert system was introduced nationally on November of 2012 by the Dutch government for the purpose of providing quick alerts and information to the citizens regarding hazardous situations or crises situations within the Dutch territory (Dutch Ministry of Justice and Security, 2012). The system is cellular tower based and is designed to be used by the authorities, who can send messages or alerts to the mobiles phones of individuals in specific areas with the help of cell towers, which can alert smartphone devices within their reach (Dutch Ministry of Justice and Security, 2020). The NL-Alert was first used on December of 2012, in a very large fire that destroyed a furniture store in the city of Tolbert in the province of Groningen (Figure 2). The authorities immediately dispatched



NL-Alert

Ontvangen: 7 aug. 04:07

NL-Alert 07-08-2018 03:50 Zeer grote brand met rook in Venlo. Ramen en deuren sluiten en ventilatie uitzetten. Nadere info volgt.

Figure 1 NL-Alert broadcast message in the area of Venlo on August 7 of 2018 after a large toxic fire broke out (source: Wikipedia)

the NL-Alert system and sent out a warning similar to the one presented in Figure 1. Through the warning, the authorities informed the surrounding area briefly, about what was happening and indicated them to keep the windows and the doors closed, and turn off any mechanical ventilation they might have turned on (Herald Veenstra, J. Haverdings, Dirk van de Kamp, M. Nuver, 2012).

Figure 2 Firefighters trying to put out the fire in a furniture shop in Tolbert, Netherlands (source: 112groningen.nl)

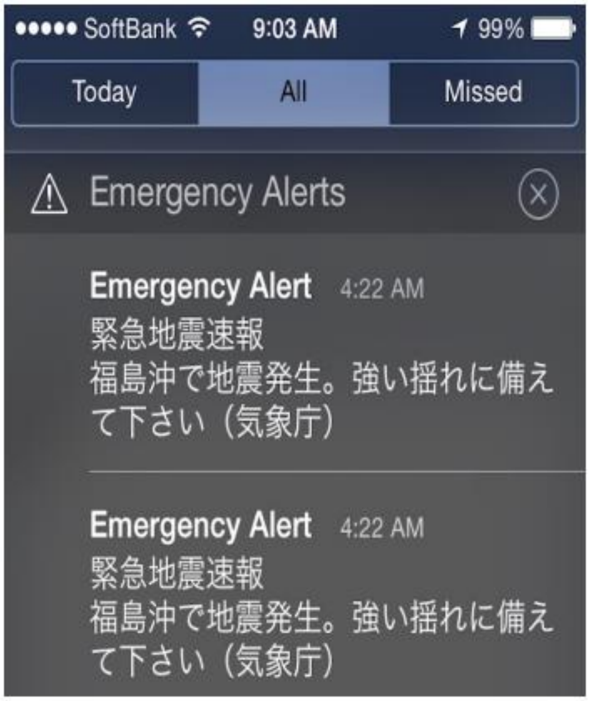
Another event that NL-Alert was used on was, when a taxi company in the city Meppel suddenly caught fire (Figure 3) on 20 of January of 2013. The area was quickly filled up with big smoke clouds and individuals around the area received the NL-Alert message from the authorities. The alert included instructions such as, what kind of measures to take in order to be safe from the smoke and any possible release of hazardous substances from the taxi company (Hilde, 2013).

Figure 3 Fire in the taxi company in the city of Meppel (source rtvdrenthe.nl)

Since its launch in 2012, NL-Alert has been activated more than 300 times (Benoît Vivier, Chris Van Arum, Håkon Straume, Amélie Grangeat, Pablo Gómez, 2019), and as of June 2020 it has been adopted by 90% of the population above the age of 12 (13.6 million) (Dutch Ministry of Justice and Security, 2020). Another fact that was observed in the behavior of the Dutch population was, that from the 10% of the people above the age of 12 that did not receive any alert message from the NL-Alert system due to various reasons, 4% of them heard it from other people. This translates to 94% of the total Dutch population above the age of 12 (14.2 million), which shows how willing people are to help each other during moments of crisis (Dutch Ministry of Justice and Security, 2020).

It is worth mentioning that, NL-Alert was amongst the first European countries that implemented the EU-Alert system domestically (European Telecommunications Standards Institute, 2019). According to the European Telecommunications Standards Institute (ETSI), the EU-Alert is the European Public Warning Service that uses cell broadcast as means of delivering public warning messages to the public. Some of the countries that are currently part of the EU-Alert along with the Netherlands (NL-Alert) are Greece (GR-Alert), Italy (IT-Alert), Lithuania (LT-Alert), Belgium (BE-Alert) and Romania (RO-Alert) (European Telecommunications Standards Institute, 2019).

2.2 J-Alert (Japan)



Emergency Alert 4:22 AM
緊急地震速報
福島沖で地震発生。強い揺れに備えて下さい（気象庁）

Emergency Alert 4:22 AM
緊急地震速報
福島沖で地震発生。強い揺れに備えて下さい（気象庁）

Figure 4 Earthquake Early Warning by Softbank in Japan (source: Japan Info website)

The J-Alert system was introduced on February 2007 by the Japan Meteorological Agency with the purpose of the quick information of the public from numerous kinds of threats such as earthquakes; volcanic eruptions; tsunamis and severe weather conditions (Centre for Public Impact, 2016). The system is satellite based and since then it has been adopted from the whole country (Centre for Public Impact, 2016). On the Tōhoku-oki earthquake of 2011, which was one of the greatest earthquakes in Japan’s history and had catastrophic consequences (Figure 5), within seconds, the Earthquake Early Warning System (EEWS) was activated and immediately, emergency alerts similar to the one presented on Figure 4, were dispatched through smart phone, TV and radio stations (Fujinawa Yukio, Noda Yoichi, 2013). The Emergency Alert was dispatched 8 seconds after the first P-wave was detected and a minute earlier before the earthquake struck giving to the Japanese population valuable time to react (Mitsuyuki Hoshiba, Kazuhiro Iwakiri, Yasuyuki Yamada, Naoki Hayashimoto, Toshihiro Shimoyama, 2011).

Individuals had time to get under their desks/tables or evacuate the buildings they were in, gas lines were shut off, and trains stopped moving (Fujinawa Yukio, Noda Yoichi, 2013).

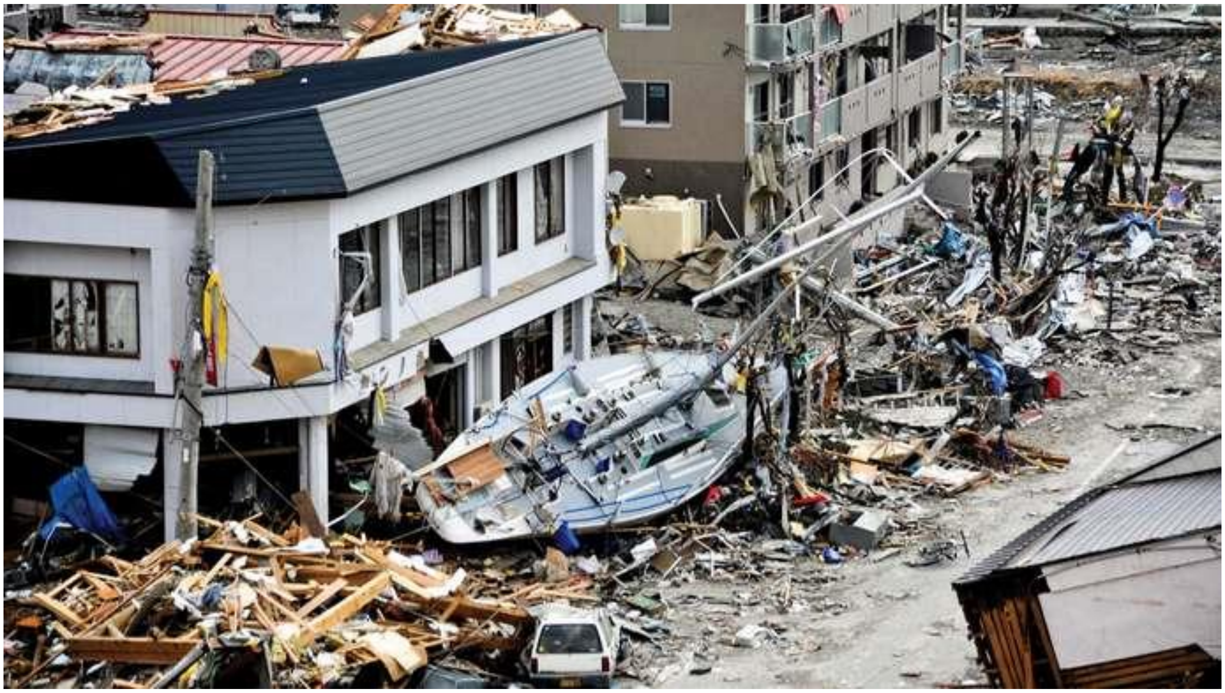
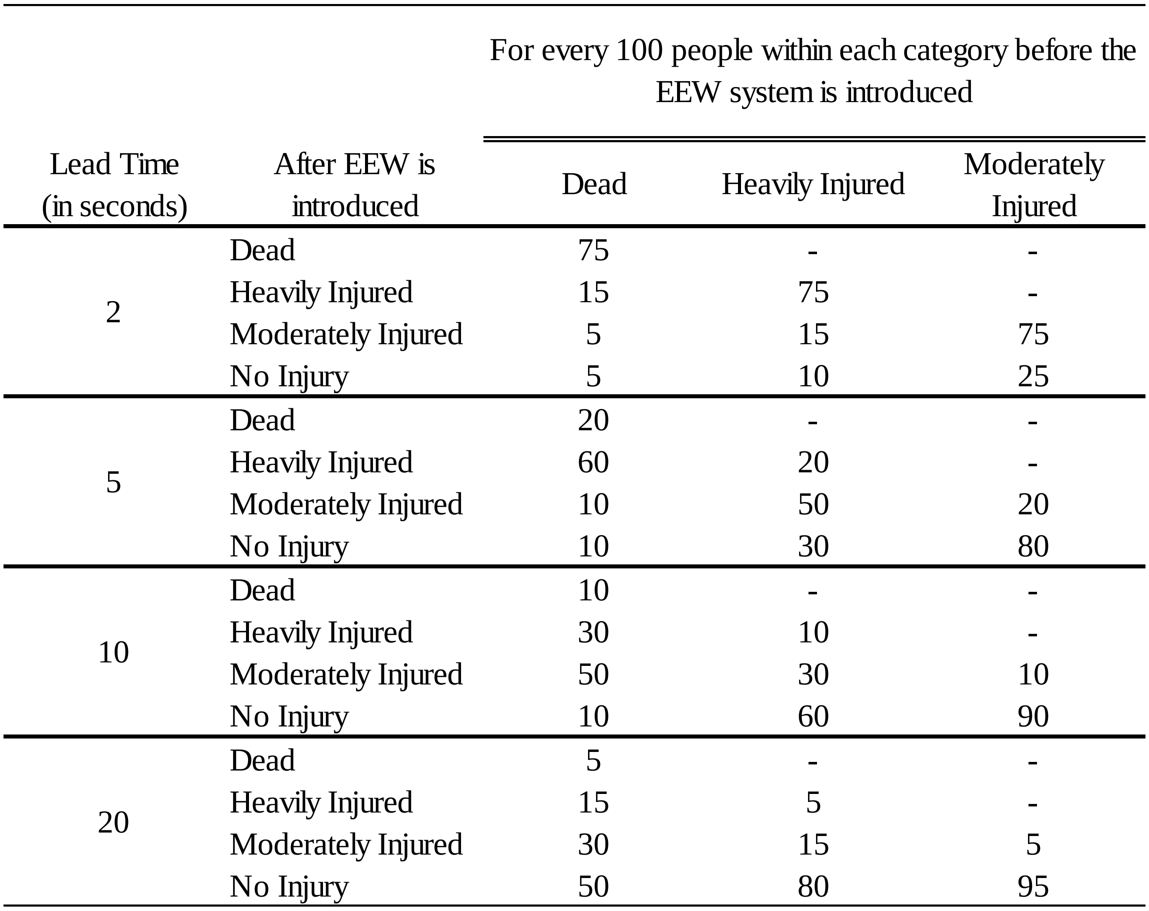


Figure 5 Aerial view of the destruction in Sendai, Miyagi prefecture, Japan, three days after being struck by the March 11, 2011, earthquake and tsunami (source Airman 1st Class Katrina R. Menchaca/U.S. Air Force photo, Encyclopædia Britannica)

Even though it is difficult to estimate how many lives were saved that day due to the Earthquake Early Warning System, a rough estimation can be made according to a tentative effectiveness table that was made by Meguro et al. (Meguro, K., Fujinawa, Y., Kawakami, N., & Nishino, T., 2004). This table (Table 1) was based on an experimental version of the Earthquake Early Warning System at a school, which tested the effectiveness of the system itself (Motosaka, M., and Homma, M., 2009). The results suggested that, a 10-second head start by the Earthquake Early Warning system could have as a result the reduction of deaths and injuries by 20% and 10% respectively, when compared to the same situation without the use of the Earthquake Early

Warning System (Fujinawa, Y., Rokugo, Y., Noda, Y., Mizui, Y., Kobayashi, M., and Mizutani, E., 2009).



		For every 100 people within each category before the EEW system is introduced		
Lead Time (in seconds)	After EEW is introduced	Dead	Heavily Injured	Moderately Injured
2	Dead	75	-	-
	Heavily Injured	15	75	-
	Moderately Injured	5	15	75
	No Injury	5	10	25
5	Dead	20	-	-
	Heavily Injured	60	20	-
	Moderately Injured	10	50	20
	No Injury	10	30	80
10	Dead	10	-	-
	Heavily Injured	30	10	-
	Moderately Injured	50	30	10
	No Injury	10	60	90
20	Dead	5	-	-
	Heavily Injured	15	5	-
	Moderately Injured	30	15	5
	No Injury	50	80	95

Table 1 Estimated reduction rate of personal suffering with the use of Earthquake Early Warning System

The table is based on the following conditions:

1) The idea that individuals could save their lives (even if they were seriously injured) within 10 seconds after having received the emergency alert

2) Individuals could be trained and educated to take the appropriate actions within 5 seconds after having received the emergency alert

3) A shaking table test indicated that people can control themselves without any upset even if the lead time is only 1 second *(Fujinawa, Y., Rokugo, Y., Noda, Y., Mizui, Y., Kobayashi, M., and Mizutani, E., 2009)*

In a survey that was conducted by the Japan Meteorological Agency (JMA), three different groups of individuals were asked to evaluate the effectiveness of the Early Emergency Warning System. The first two large sample groups (EEWg and EEWa, approximately 2000 individuals) experienced the seismic shaking the least and the smaller group (S-Tohoku, approximately 820 residents) experienced the shaking the most.

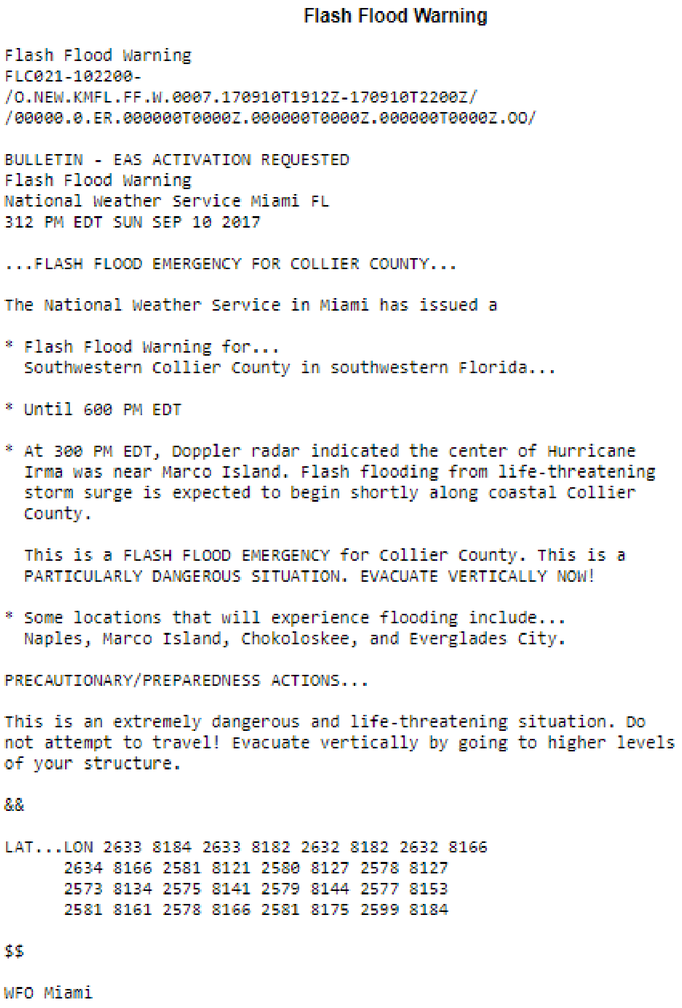
	Useful	Somewhat Useful	Somewhat Useless	Useless
EEWa	28%	54%	15%	3%
EEWg	38%	53%	8%	2%
S-Tohoku	47%	43%	8%	2%

Table 2 Rate of satisfaction for the present state of the Earthquake Early Warning System

The results showed that all three groups, found the Earthquake Early Warning System to be highly effective given the fact that the sum of the percentages of the favorable responses (1 or 2) were above 80% for all three groups, and in some cases above 90%. On the other hand, the percentage of dissatisfaction of the Earthquake Early Warning System was expressed by the two unfavorable responses (3 or 4), which were below 20% for all three groups (Yukio Fujinawa, Yoichi Nodab, 2013).

2.3 Flash Flood Emergency Alert (USA)

On September 10 of 2017, the National Weather Service (NWS) along with the National Hurricane Center (NHC) issued warnings for flash floods in several areas of the state of Florida due to landfalls that had been caused by Hurricane Irma, a category 4 hurricane (Figure 7). The warnings were distributed by the National Weather Service through their website, Facebook, radio, TV, SMS messages and Twitter. The residents of those areas were asked to evacuate either vertically by moving to the highest level of the building that they were living in or totally, and were urged not to travel but instead stay safe during this natural phenomenon as seen on Figure 6.

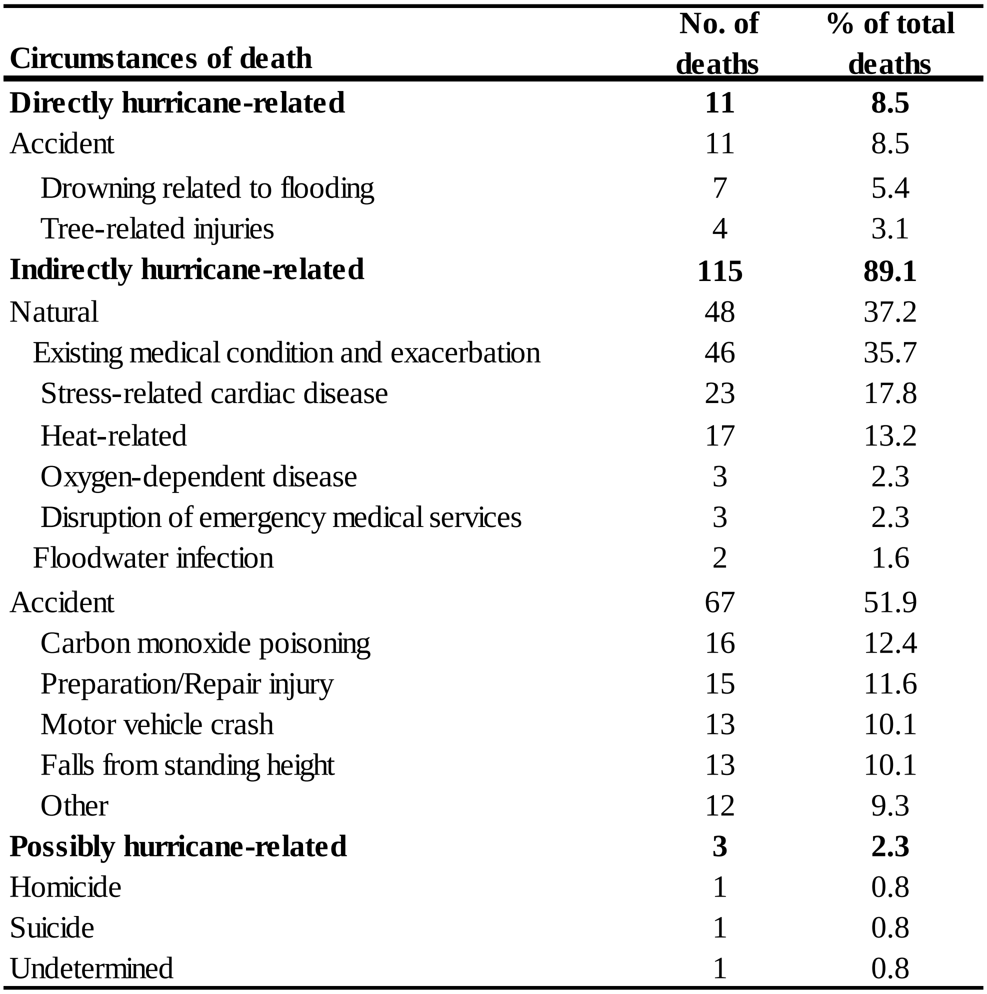


Flash Flood Warning

```
Flash Flood Warning
FLC021-102200-
/O.NEW.KMFL.FF.W.0007.170910T1912Z-170910T2200Z/
/00000.0.ER.000000T0000Z.000000T0000Z.000000T0000Z.OO/

BULLETIN - EAS ACTIVATION REQUESTED
Flash Flood Warning
National Weather Service Miami FL
312 PM EDT SUN SEP 10 2017

...FLASH FLOOD EMERGENCY FOR COLLIER COUNTY...

The National Weather Service in Miami has issued a

* Flash Flood Warning for...
  Southwestern Collier County in southwestern Florida...

* Until 600 PM EDT

* At 300 PM EDT, Doppler radar indicated the center of Hurricane
  Irma was near Marco Island. Flash flooding from life-threatening
  storm surge is expected to begin shortly along coastal Collier
  County.

  This is a FLASH FLOOD EMERGENCY for Collier County. This is a
  PARTICULARLY DANGEROUS SITUATION. EVACUATE VERTICALLY NOW!

* Some locations that will experience flooding include...
  Naples, Marco Island, Chokoloskee, and Everglades City.

PRECAUTIONARY/PREPAREDNESS ACTIONS...

This is an extremely dangerous and life-threatening situation. Do
not attempt to travel! Evacuate vertically by going to higher levels
of your structure.

&&

LAT...LON 2633 8184 2633 8182 2632 8182 2632 8166
      2634 8166 2581 8121 2580 8127 2578 8127
      2573 8134 2575 8141 2579 8144 2577 8153
      2581 8161 2578 8166 2581 8175 2599 8184

$$

WFO Miami
```

Figure 6 Flash Flood Warning issued for the Southwestern Collier County by the National Weather Service Weather Forecast Office of the state of Miami (source: National Weather Service archive)

Hurricane Irma affected 7 million residents in the state of Florida (Centers for Disease Control and Prevention (U.S.), 2018). According to the Morbidity and Mortality Weekly Report (Centers for Disease Control and Prevention (U.S.), 2018), in the states of Florida, Georgia and North Carolina, which were affected by Hurricane Irma, there were in total 129 deaths of which 11 of them were directly related to the hurricane and the rest were indirectly related to it. As shown on Table 2 below only seven deaths were caused by drowning, which indicates that the warnings by the National Weather Service (NWS) for flash flooding were lifesaving for many people (Centers for Disease Control and Prevention (U.S.), 2018).



Circumstances of death	No. of deaths	% of total deaths
Directly hurricane-related	**11**	**8.5**
Accident	11	8.5
Drowning related to flooding	7	5.4
Tree-related injuries	4	3.1
Indirectly hurricane-related	**115**	**89.1**
Natural	48	37.2
Existing medical condition and exacerbation	46	35.7
Stress-related cardiac disease	23	17.8
Heat-related	17	13.2
Oxygen-dependent disease	3	2.3
Disruption of emergency medical services	3	2.3
Floodwater infection	2	1.6
Accident	67	51.9
Carbon monoxide poisoning	16	12.4
Preparation/Repair injury	15	11.6
Motor vehicle crash	13	10.1
Falls from standing height	13	10.1
Other	12	9.3
Possibly hurricane-related	**3**	**2.3**
Homicide	1	0.8
Suicide	1	0.8
Undetermined	1	0.8

Table 3 Circumstances of confirmed deaths related to Hurricane Irma — Florida, Georgia, and North Carolina, September 4–October 10, 2017

By examining better the reasons behind the hurricane related deaths, we can imply that the human behavior played a severe role in them. In conformity with the case study mentioned in the report Understanding Evacuee Behavior: A Case Study of Hurricane Irma (Wong, S., Shaheen, S., & Walker, J, 2018), a sample of 645 people that were affected by Hurricane Irma were asked a line of questions regarding their behavior during the event. As shown on Table 4, almost 70% of the people that received the evacuation order evacuated their place or residence, whereas the rest 30% did not. When it came to the part of the sample that did not receive any mandatory orders, 46.4% of them decided to evacuate their place of living whereas the rest 53.6% decided to stay in their property (Wong, S., Shaheen, S., & Walker, J., 2018).

		Evacuation Decision	
		Yes	No
Received Mandatory Order	Yes	69.50%	30.50%
	No	46.40%	53.60%
	Total	57.10%	42.90%

Table 4 Bivariate Cross Tabulation for Evacuation Decision and Mandatory Order

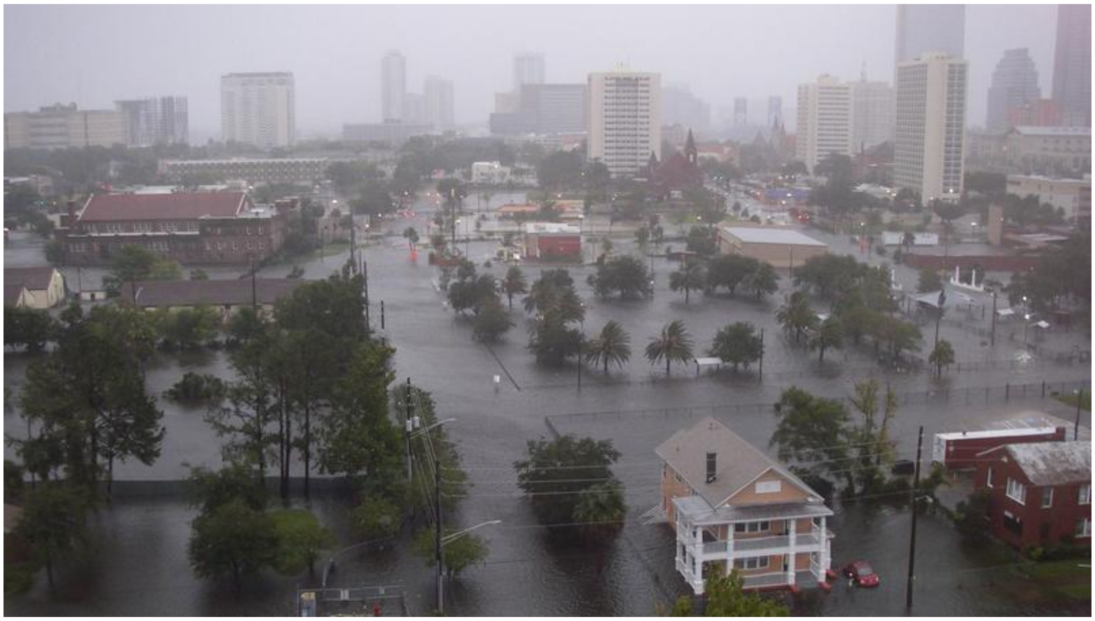


Figure 7 Flooding in Jacksonville during Hurricane Irma (source: news.wjct.org)

As seen on the table below (Table 5), where the reason behind the decision making of each respondent is studied on a deeper level, almost 50% of the respondents that did not evacuate their place or residence, did so because they did not want to leave their property. By taking into account also, the percentage of the respondents that did not receive any evacuation orders, which was 15.9%, we can interpret that the reason behind the deaths directly related to Hurricane Irma were not due to the ineffectiveness of the alert system but rather a product of human error (Wong, S., Shaheen, S., & Walker, J, 2018).

Multiple selection allowed

Reasons to Travel Far Distance Out of County (n=368)	
I felt my home wasn’t safe for this storm and that’s how far I had to go to reach safety	38.90%
That was the location of the friend/relative I wanted to stay with	37.20%
I stayed in the county	17.70%
Because my location was ordered to evacuate the county	17.10%
That’s how far I had to go to find available hotel/motel/public shelter or other location to stay	16.20%
Other	18.20%
Reasons to Not Evacuate (n=277)	
Didn't want to sit in traffic	49.10%
Didn't want to leave	48%
Wanted to protect my property	34.70%
Didn’t want to go to public shelter	31.40%
Believed the storm would not be bad	29.60%
Some requirement to go to work during storm	21.70%
Was not sure where I could take my pets	18.10%
Didn't receive any orders	15.90%
Didn't have the money to evacuate	14.40%
No friends or family to shelter with	6.10%
Tried to but ended up going back home due to traffic	2.50%
Tried to but was turned away at shelter	0.40%
No transportation to get to shelter	0.00%
Other	37.50%

Table 5 Respondent Reasons for Traveling Far Distance and Not Evacuating

Chapter 2: Design of the application

2.1 Logo Design

The logo is the first thing someone notices about an application from the very first moment that the application is downloaded on his smartphone device, therefore it should communicate some kind of message to the user whether that is, by the use of proper colors or symbols on the logo that indicate what the application is in the first place. This means that, for a logo to be effective and memorable to the user it should be composed by elements that create the desired association in the user's mind. In the instance of the application that it is being presented on this thesis, the colors, the symbols as well as the name were taken into consideration for the design of the logo (see Figure 1).

Firstly, a darker tint of the color red was chosen for the background and part of the symbol of the application. The reason behind this decision, was that it was deemed important to associate the application itself with fire and danger on the user's mind, so that in the instance where a fire related incident occurred, this application would be among the first things that would come to the user's mind. Furthermore, it was decided for the application to have a minimalistic and uncongested design in order to achieve simplicity and avoid having any unnecessary elements which could end up creating a sense of confusion to the user. Moreover, it was decided that the size of the symbol in the logo should be larger than

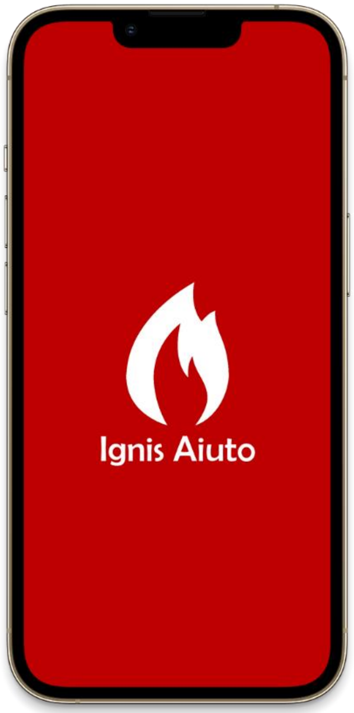


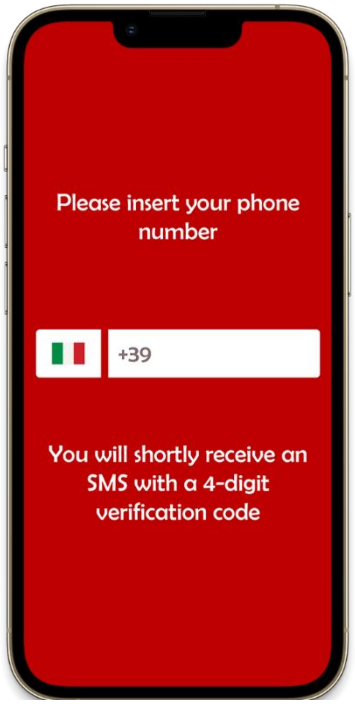
Figure 8 Logo of the application

average so that users that are of older ages or users that have poor eyesight can distinguish the elements of the application.

Other elements of the logo of the application that were taken into consideration were the symbol and the name of the application itself. As it can be seen in Figure 1, the symbol on the logo is a flame composed by the same tint of the color red as in the background and the color white. This was done in order to create contrast between the symbol and the background making it easier for people that have poor vision or are of older ages to be able to distinguish this particular application from any other application they might have on their smartphone device. Last but not least, on the same image the name of the application can be seen below the flame symbol, the name is Ignis Aiuto. The name is composed of two different words, the Latin word Ignis which in the English language can be translated as fire and the Italian word Aiuto which can be translated as help.

2.2 Registration of the user to the application

The first time the user downloads and opens the application, he will be greeted with the screen presented on Figure 2. In this screen, the user will be asked to select the dialing code of his country by tapping on the flag section of the screen. Based on the geographical location of the user, the application will automatically have by default the flag of the country that the user is currently located, making the registration process easier. In the instance that the user’s sim card does not have the dialing code that is selected by default but the dialing code of another country, he can simply change the country by tapping on the flag. In that case, a drop


Please insert your phone number

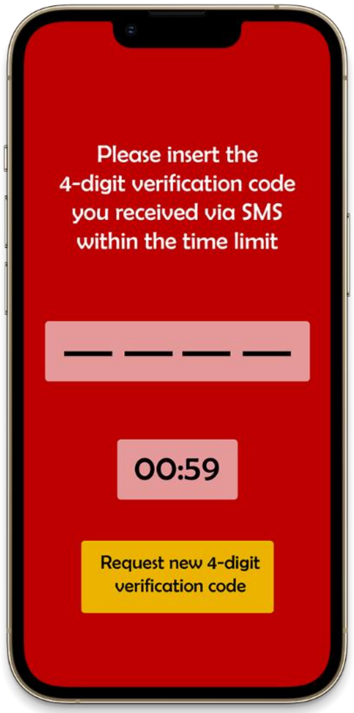
+39

You will shortly receive an SMS with a 4-digit verification code

Figure 9 Registration Screen

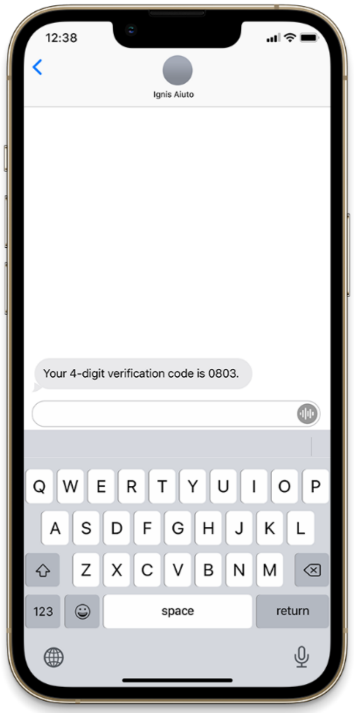
down menu will show up where the user can scroll down or up in order to find the dialing code of his sim card.

During the next step, the user will have to input his 10-digit mobile phone number in order to receive a 4-digit verification code. After the user inserts his mobile phone number, he will be redirected to the screen presented on Figure 3. On this screen the user will be asked to insert a 4-digit code that will be sent to him via SMS. This step is necessary because its purpose it to verify that the user has inserted his own mobile phone number and not a false or fictitious one. By doing so, the smartphone device is tied to the mobile number that has been inserted and by extension to the user himself, with the goal of discouraging in this way malicious intents.



Please insert the 4-digit verification code you received via SMS within the time limit

Figure 10 Verification Screen



Your 4-digit verification code is 0803.

Figure 11 4-digit verification code sent out by the API to the user

The way the verification step functions when it comes to the technical aspect, is by the use of a verification API. API stands for Application Programming Interface, and its purpose is to be the intermediary between the application itself and the server that is hosting the application. In this instance, the server would generate a 4-digit verification code and send it to the user via SMS (see Figure 4), then the verification API would compare the 4-digit code that the user input with the one generated by the server. If the 4-digit verification code that the user input matches the one that the server generated then the verification step would be completed successfully, otherwise, the verification step would fail and the user would be prompted to try again or request a new 4-digit verification code. Another layer of protection that should be implemented during the verification process is the addition of a one minute timer. The user has to input the 4-digit verification code within the time limit, else, the 4-digit verification code will not be valid anymore and the user will not be able to make his registration successfully and as a result, he would have to request a new 4-digit verification code. The purpose of this feature is to discourage users from adding a fictitious phone number and then trying to guess the 4-digit verification code in hopes of getting through the verification process without using any real data. Usage of verification APIs is one of the most widespread ways to create a two factor authentication, applications like Whatsapp use verifications APIs to verify their users when they first sign up (see Figure 5). These APIs provide an extra layer of security by verifying that the users are who they say they are.

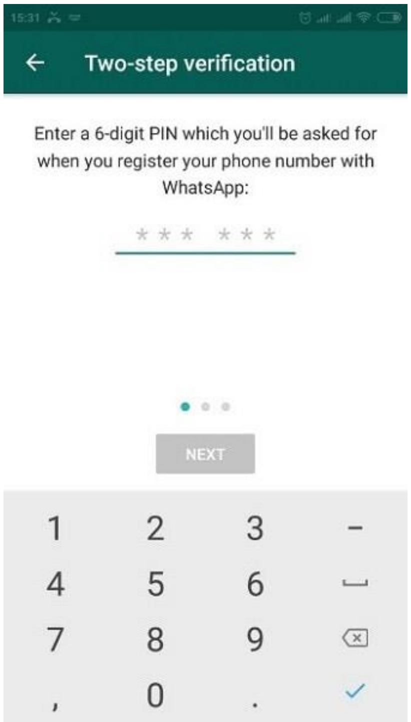

Enter a 6-digit PIN which you'll be asked for when you register your phone number with WhatsApp:

Figure 12 Whatsapp verification API requesting from the user a 6-digit code in order to verify the user (source: https://drfone.wondershare.it/whatsapp/whatsapp-business-code.html)

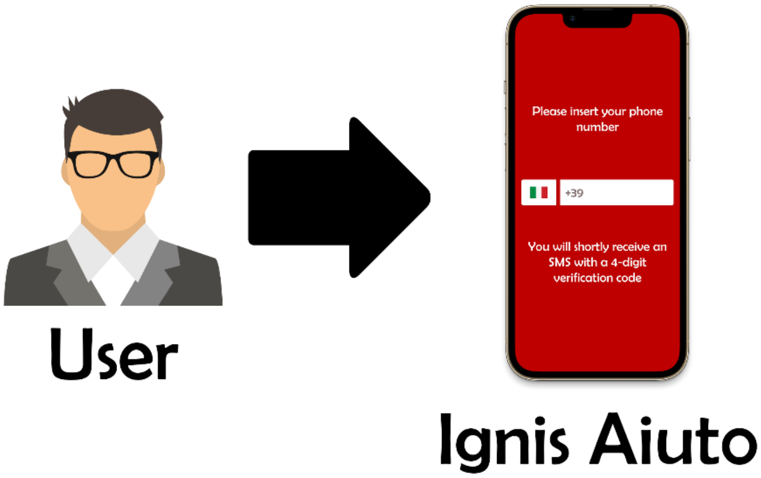
This procedure will be mandatory for the user in order to continue using the application, and it will be done only once during the first time of the registration of the user or until the user changes the sim card on his smartphone device. In that case, the user would have to go through this procedure again in order to register the new sim card for the application.

In order for the verification to be completed, the verification process is divided into two stages where each one of them requires the API to be called. Those two stages are called verification request and verification check. To make the understanding of how the verification API functions clearer, below the procedure will be presented via visual assistance.

Verification Request:

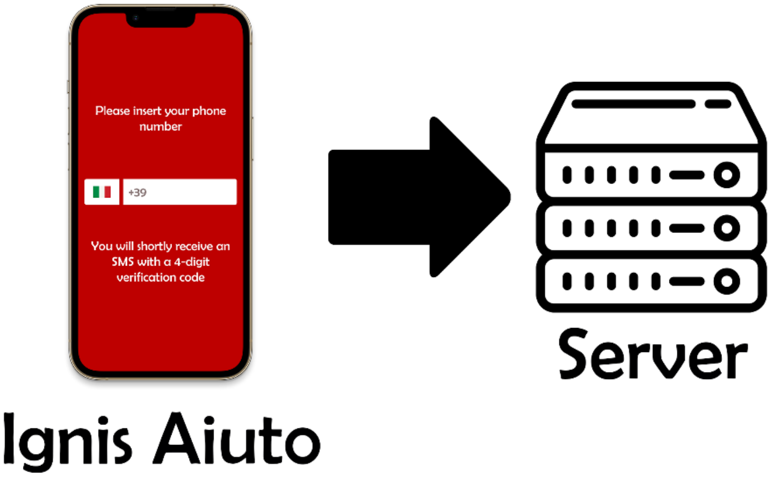
Step 1

The user decides to register for the services of Ignis Aiuto via the application by providing his phone number in the registration screeen.


User
Please insert your phone number
+39
You will shortly receive an SMS with a 4-digit verification code
Ignis Aiuto

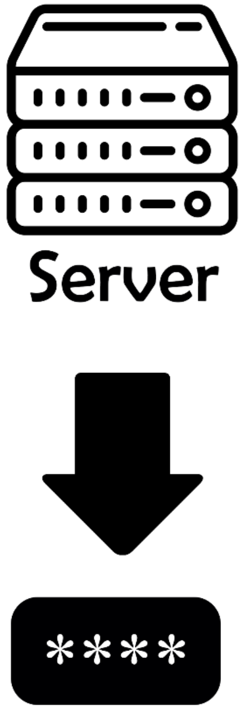
Step 2

In order to confirm that the user indeed has acess to the phone number the inserted on the previous step during the registration, the application makes an API call to the server.


Please insert your phone number
+39
You will shortly receive an SMS with a 4-digit verification code
Ignis Aiuto
Server

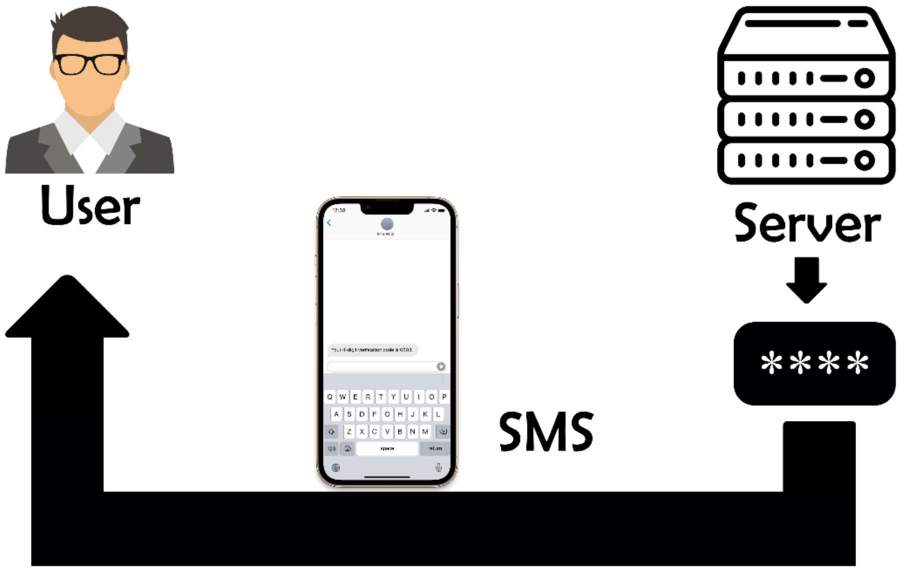
Step 3

The verification API will generate a 4-digid code which will be linked to the user that just registered. This means that, in order for that user to pass the verification process sucessfully, he will have to use only the 4-digit code that has been linked to his registration attempt.



Step 4

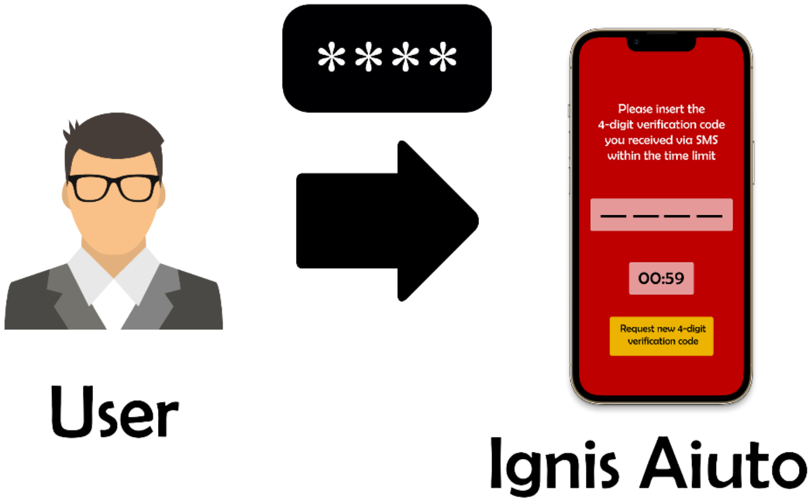
The server then through the verification API will attempt to send the 4-digit code to the user via SMS.



Verification Check:

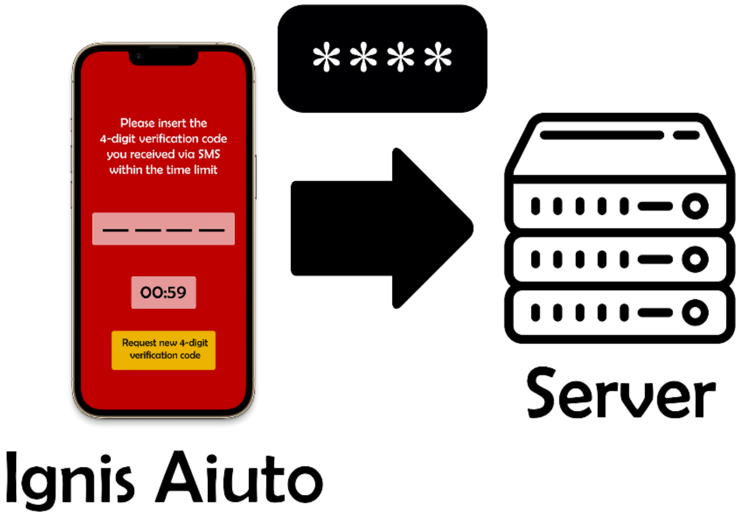
Step 5

The user will then enter the 4-digit code he received on the verification screen within the 1 minute time limit.


****
Please insert the 4-digit verification code you received via SMS within the time limit
— — — —
00:59
Request new 4-digit verification code
User
Ignis Aiuto

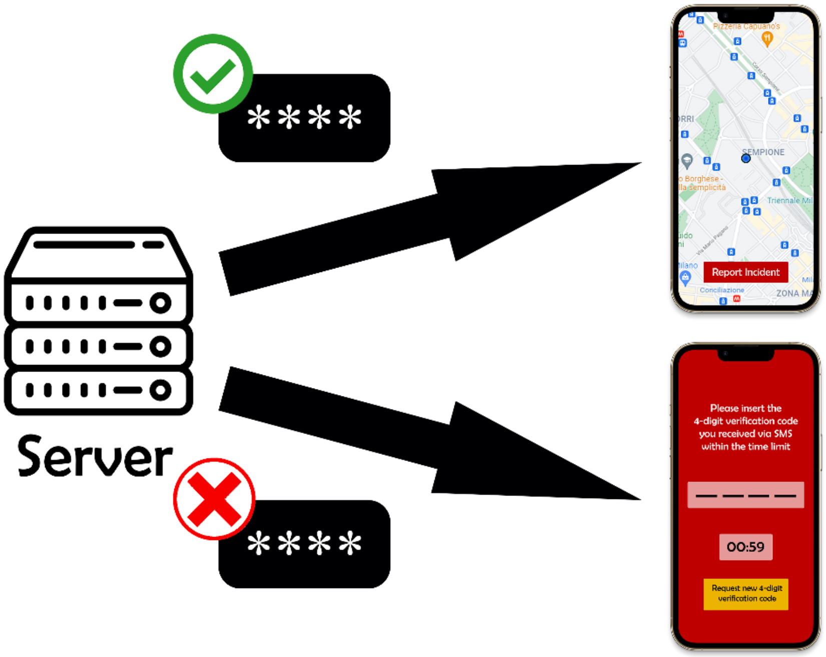
Step 6

The application will make an API call to the server, passing in the user’s phone number along with the 4-digit code the user insterted.


Please insert the 4-digit verification code you received via SMS within the time limit
— — — —
00:59
Request new 4-digit verification code
****
Server
Ignis Aiuto

Step 7

The API will check wether the 4-digit code that was inserted matches the one that was sent or not. If it matches, then access to the main interface of the application will be granted, if it does not, the user will have to go through the verification process again.


****
Server
****
Report Incident
Please insert the 4-digit verification code you received via SMS within the time limit
00:59
Request new 4-digit verification code

2.3 How the application works from the user’s point of view

2.3.1 What already exists

Before we start explaining how the application would look like from the user’s perspective, it is worth mentioning what already exists in the market and how it operates in comparison to Ignis Aiuto. A good point to start, would be the application “112 Where Are U”, an emergency application linked to the 112 European Union Public Safety Answering Point (PSAP) which was created in collaboration with Regione Lombardia, Regione Lazio and Ministero Dell’Interno and its purpose of existence is to allow the user to contact rescuers in emergency situations by sending their position to a monitoring unit or calling them through the application by the use of the European Emergency Number 112, who then will dispatch help immediately. The user can choose himself to ask for help from the police, the fire department or an ambulance.

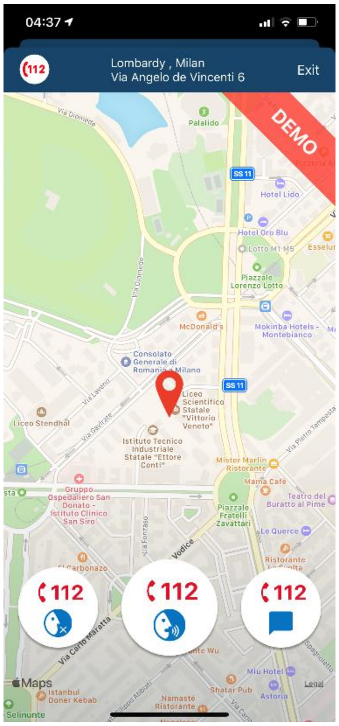
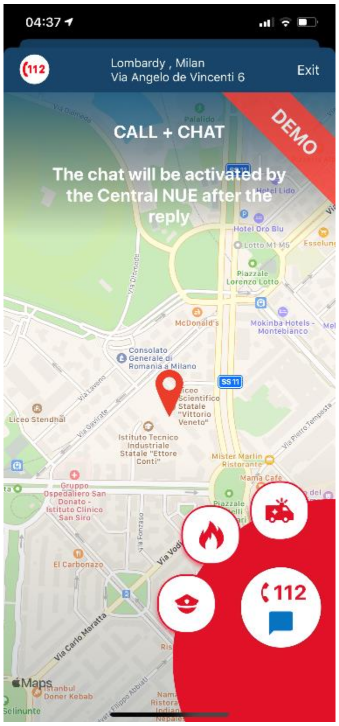


Figure 13 Main Screen of the (Demo version of the) application 112 Where Are U

To further investigate the method that the application operates as well as to find similarities with the application that is being presented on this thesis, the Demo function of 112 Where Are U was used. The Demo function simulates how the procedure would unfold in the instance that the user used the application to call for an emergency. The Demo function was used with my personal phone number and device for the needs of the simulation.

On Figure 12, the main user interface can be seen as well as what are the options for the user. There are 3 options, the "Silent Call" option where the user can call an operator in the instance where he cannot talk due to any reason, the "Voice Call" option where the user can normally talk with an operator and explain what is exactly the situation and the "Call + Chat" option where the user can chat with an operator and request the necessary help. Another thing that can be seen on the main screen of the application, is the map of the general area of the user as well as his estimated location which is being represented with the red marker. Judging by the location that is being presented on the map and my true current location when using the application, it can be said that there is a small inaccuracy of about 20-30m from the location presented on the application and my true location which in the case of an emergency would not be a huge issue.



Lombardy , Milan
Via Angelo de Vincenti 6

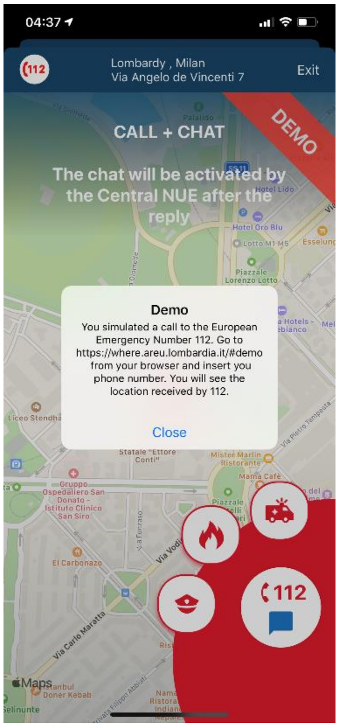
CALL + CHAT

The chat will be activated by the Central NUE after the reply

Figure 14 Emergency Request Options on the application 112 Where Are U

On Figure 13, we can see what options the user has when it comes to an emergency request. The user here can request from the operator the assistance of an ambulance, the fire department or even the police department. By tapping in any of the 3 options the user will come into contact with an operator and provide further information. These are the steps that someone would have to follow in order to request help from the application.

Apart from the user's point of view, the Demo function of the application can provide us also with what the operator would see in the instance the application was used. On Figure 14, the Demo function of the application provides us with a message which informs us about what the operator would see exactly. By following the https://where.areu.lombardia.it/#demo address we get redirected to the main website of the application "112 Where Are U". In order to view the operator's point of view we are asked to input the phone number that was used during the Demo version, in this instance my personal phone number (see Figure 15), part of the phone number was covered for obvious reasons.



Lombardy , Milan
Via Angelo de Vincenti 7

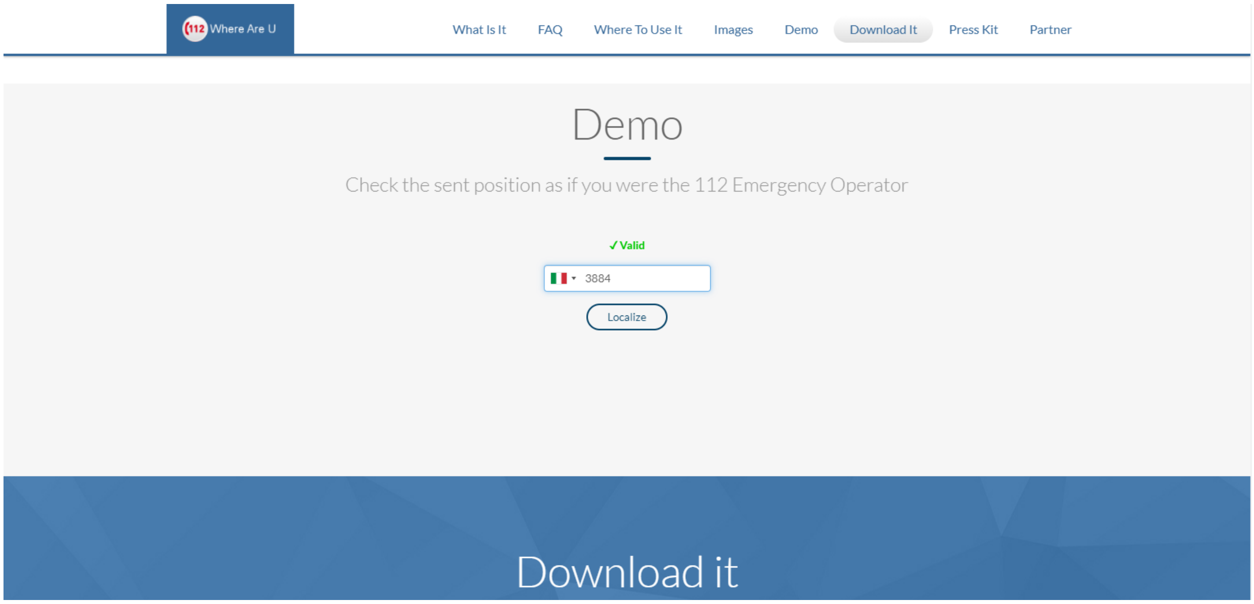
CALL + CHAT

The chat will be activated by the Central NUE after the reply

Demo

You simulated a call to the European Emergency Number 112. Go to https://where.areu.lombardia.it/#demo from your browser and insert you phone number. You will see the location received by 112.

Figure 15 Message from the Demo function of the application 112 Where Are U



Demo

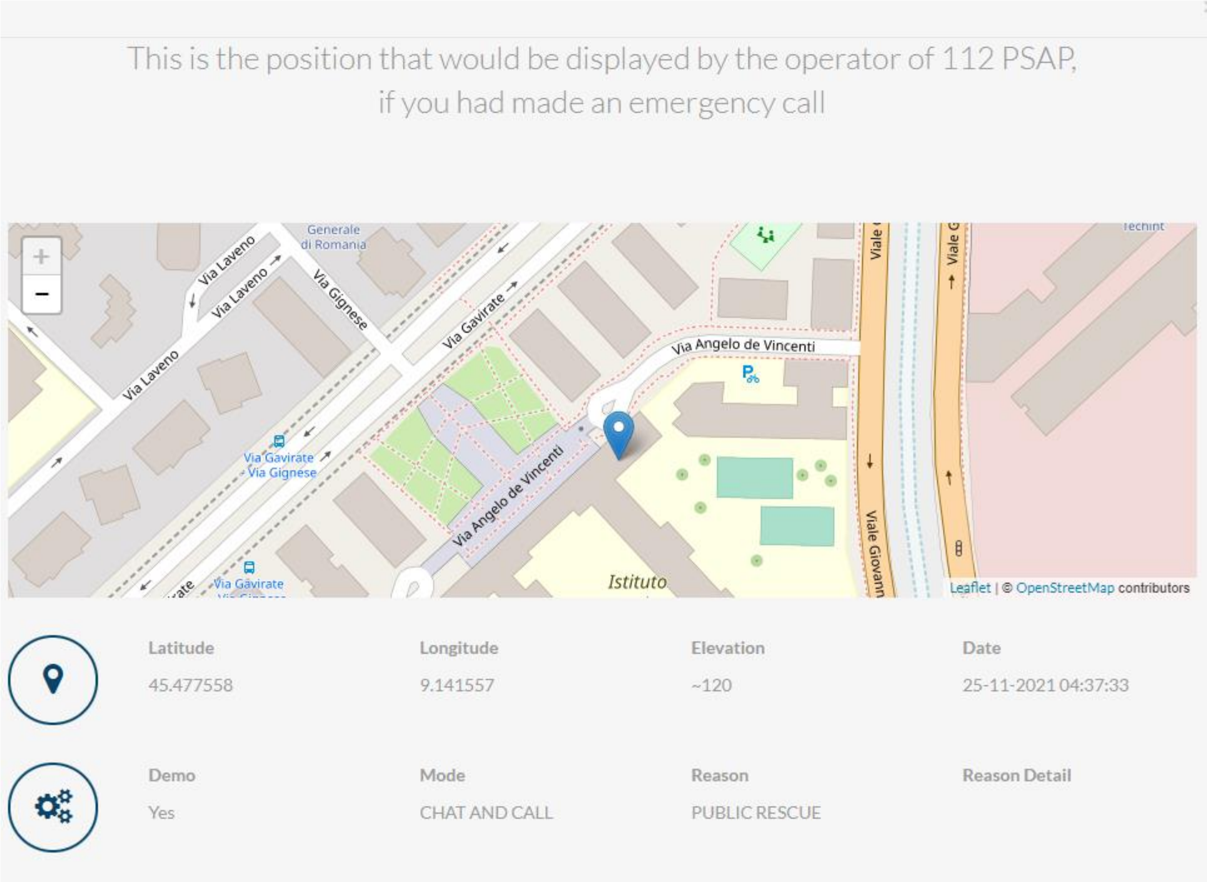
Check the sent position as if you were the 112 Emergency Operator

✓ Valid

3884

Download it

Figure 16 Position sent by the user to the Emergency Operator via the application 112 Where Are U



This is the position that would be displayed by the operator of 112 PSAP, if you had made an emergency call

Latitude	Longitude	Elevation	Date
45.477558	9.141557	~120	25-11-2021 04:37:33

Demo	Mode	Reason	Reason Detail
Yes	CHAT AND CALL	PUBLIC RESCUE	

Figure 17 Position displayed by the Emergency Operator of the application 112 Where Are U

After inputting the phone number, the website displays with a green tick the validity of the number and the fact that I am already a registered user in the system. By clicking on the "Localize" button, we get redirected to the screen that an operator of the emergency number 112 would see (see Figure 16). In this image we can see that the operator would see information such as the exact coordinates that were registered by the application, the elevation as well as the time and date that the emergency was requested by the user through the application. Furthermore, the operator can also see the kind of help we requested as well as any further details that we might have given to him during a call or message exchange through the application.

2.3.2 Ignis Aiuto

Now that we saw what already exists in the market when it comes to requesting assistance during emergencies as well as the way it operates, we will see what the approach of Ignis Aiuto will be and what steps the user will have to take in order to achieve the desired result by using the application.

After the user has registered successfully on the application, he will be able to use it in order to report any fire related incidents whenever he wants just by the use of the application on his device. On this part of the subchapter, we are going to see how the application will function in the instance that a user wants to report a fire related incident and what procedure will be followed after that. As soon as the user opens the application after having completed the registration, he will be greeted with a map of the area where he is located along with his specific location (see Figure 6). The user will be displayed with a blue dot on the screen, while on the background there will be a map that will be displaying the general location of the user that has been retrieved from Google Maps Platform. On the bottom of the screen there will be located the “Report Incident” button.

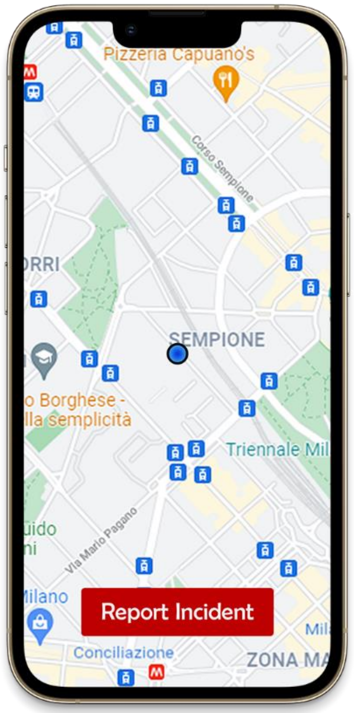


Figure 19 Main Screen/Report Incident Screen

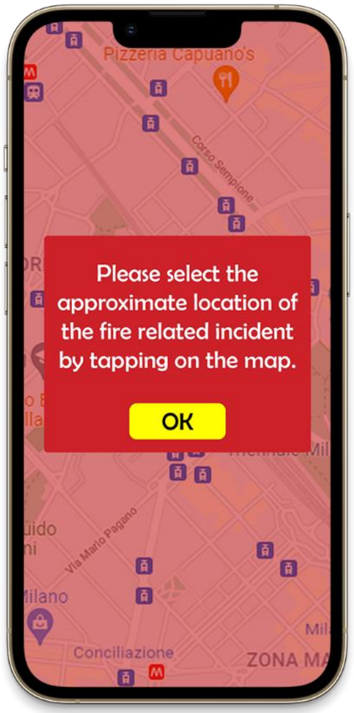

Please select the approximate location of the fire related incident by tapping on the map.

Figure 18 Select Location Screen

By tapping on the “Report Incident” button, the user will have the ability to report a fire related incident. By doing so, the user will be redirected to the screen presented on Figure 7.

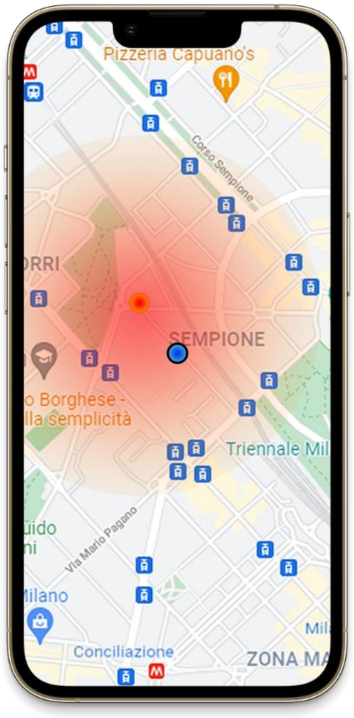
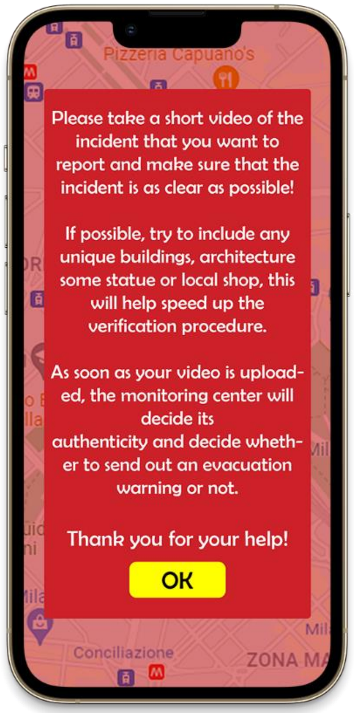


Figure 20 Screen of the application after the user has reported a fire related incident

Here, the user can read a message that will be explaining to him what he has to do next in order to proceed with the report submission. In this instance, the user is prompted with the message that is requesting him to choose the approximate area that he thinks the event is taking place by simply tapping on the map. On Figure 8, we can see how the screen would look like after the user completed the previous step. Here, the user can be seen on the screen as a blue dot again, while the incident that was reported by him, is being displayed by an orange dot with a red "aura" around it. The purpose of the orange dot is to display the location that the user selected, whereas the purpose of the red "aura" around the orange dot is to display an estimate area that could potentially be affected by the fire incident over time.

In an ideal world, where people have no malicious intents and look after one another, these steps would be more than enough in order to trigger the deployment of warning messages and help save many lives. Unfortunately though, we do not live in such ideal world, we live in a world where people that have malicious intents try to abuse the system and use it to their advantage while exploiting other people. An issue that can occur by following these steps so far, is the ease with which someone could submit a false fire related incident. Even though some measures have been taken in order to discourage such misuse of the application (see Figure 10 and Figure 11), after extended thought, they were deemed not enough in order to provide the smooth and safe use of the application. Having said these, it was decided to add a further step for the incident verification on the application after the user has selected the location of the incident (see Figure 9). That step is to ask the user to take a short video of the incident which then will be automatically sent to a monitoring unit, which will decide the authenticity of it, based on the location and the surrounding environment that the user has reported the incident. The monitoring unit, could be consisted of several individuals appointed by Dipartimento della Protezione Civile or, the Civil Protection Department of the respective country that wants to use this application on its own territory, and could operate under the same department at all times. Apart from the location and the surrounding environment, the monitoring unit would also have to judge the authenticity of the video based on the time that the video was taken as well as by judging the metadata of it. Metadata can be defined as a set of data



Please take a short video of the incident that you want to report and make sure that the incident is as clear as possible!

If possible, try to include any unique buildings, architecture some statue or local shop, this will help speed up the verification procedure.

As soon as your video is uploaded, the monitoring center will decide its authenticity and decide whether to send out an evacuation warning or not.

Thank you for your help!

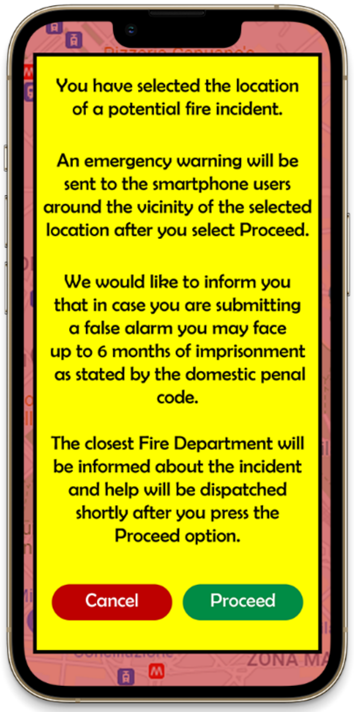
OK

Figure 21 Screen of the application where the user is asked to take a video of the fire related incident he wants to report

that describes and gives information about other data, in the instance of a video file, metadata could be the location that the video was taken, the characteristics of the device that took the video along with the exact time the video was taken.

In order to perceive exactly how this monitoring unit would function we can take as an example modern security systems that have video alarm verifications. The way a video alarm verification works is by having ones security system paired with an alarm monitoring center. In the instance that the alarm is triggered, individuals at the monitoring center could view the security camera footage and check what exactly caused the alarm to be activated. After having verified that indeed someone with malicious intents triggered the alarm, the next step is to call the local authorities and provide any essential information for the incident itself. By doing so, it is ensured that there is quick and accurate emergency response by the authorities helping to protect the customer that has his security system connected to that monitoring unit as well as his property and belongings.

The next steps that the user will have to follow after the video has been uploaded are presented on Figure 10 and Figure 11. Here the user will be prompted to a screen where a warning message will appear. In this message, a brief explanation will be given to the user of what will happen after the video has been uploaded. In addition to this, and given all the security measures that have been discussed so far for the avoidance of the misuse of the application, another extra layer of protection will be taken. In order to discourage any malicious use of the application, the user will be warned that in case he submits a false warning, as stated by the domestic penal code, he could face up to 6 months of imprisonment. According to Bradley et al. when an individual knows what the punishment of his action will be, he is less likely to commit a crime than if he did not (Does The Perceived Risk Of Punishment Deter Criminally Prone Individuals? Rational Choice, Self-Cotrol, And Crime, 2004). In the instance where the user wants to proceed with the submission of the report he will be prompted to yet another verification screen (see Figure 11) where again he will be asked if he is certain that he wants to proceed with this report while also being reminded again about what the domestic criminal code states.



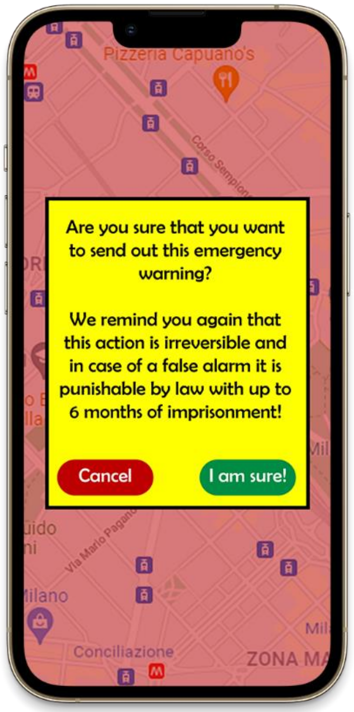
You have selected the location of a potential fire incident.

An emergency warning will be sent to the smartphone users around the vicinity of the selected location after you select Proceed.

We would like to inform you that in case you are submitting a false alarm you may face up to 6 months of imprisonment as stated by the domestic penal code.

The closest Fire Department will be informed about the incident and help will be dispatched shortly after you press the Proceed option.

Figure 23 Warning Screen of the application where the user is informed about what will happen next



Are you sure that you want to send out this emergency warning?

We remind you again that this action is irreversible and in case of a false alarm it is punishable by law with up to 6 months of imprisonment!

Figure 22 Second Warning Screen of the application informing the user about the penalty in case of submission of a false fire incident

This is the last thing that the user will have to do in order to conclude with the incident submission. After this point is up to monitoring unit to decide on how to proceed further with the submitted report. At this point, the monitoring unit will know the exact location of the user when he submitted the incident, the exact location of the incident that the user chose on the map as well as his phone number where if the report turns out to be false they can further pursue with investigations and criminal charges.

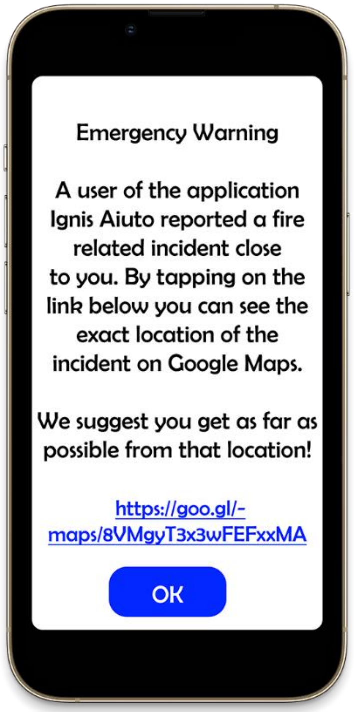
2.4 How the application works from the operator's point of view

Now that the user's aspect has been discussed as well as what he has to do in order to use the application effectively, we are going to discuss what would happen next from the operator's point of view in the instance of an event. We are going to see in detail what the operator would have to do in the instance of an incident in addition to all the steps that he would have to take in the shortest time possible in order to provide the most efficient and effective response to the fire incident reported by the user of Ignis Aiuto.

Initially, the operator would see on his screen an image similar to the one presented in Figure 16, along with the file of the video recording that the user took from the incident and uploaded during the submission step. Judging by the metadata of the video file, the recorded location of the user by the application when he recorded the video, the area that the user recorded with his phone as well as the general location of the area, the operator would have to determine the authenticity of the video and the submission request. Given the recording point of view, the operator would have first to determine the precise location that the user took the video on the map in order to be able to analyze what he is seeing in the video. Any unique buildings, architecture or even some statue or local shop could speed up this process by a lot. Next, the operator would have to verify that there is a correspondence between the light on the background of the video and the timing of the video that was reported by the user. For example, if a user submits a video with a fire incident taking place in the middle of Milan in the middle of the night but on the video submission the operator sees daylight on the background, then that video is most likely a false alarm and the user will be investigated by the police and will furthermore be charged with a criminal offense. As mentioned above, the operator would have also to cross-check the metadata of the video file submitted in order to verify the authenticity of the submitted report. For instance if the operator notices on the metadata that the video file has a date other than the current one, then most likely that video is a fake one which was either digitally modified in order to give to the operator the illusion that an incident is indeed taking place in real time or it is a video from a past event. In the scenario that the operator or the team of operators receives many submission requests by different phone numbers for the same location within a short time period, then that incident would be deemed as a legit request and thus the operator or the team of operators would proceed to the next step.

Having said all these, if everything has been cross-checked and seems to be legit, then the operator(s) would move forward to the next step. The next step, is to send out warning messages to individuals around the vicinity of the reported event. The application itself offers by default a suggested radius which is represented by the red “aura” as mentioned earlier, but the operator could judge by himself how large the incident is in reality and the amount of people he would have to warn in order save as many people as possible in the shortest time possible.

In order to send out these warning messages, a series of steps would have to be followed by the operator(s). These steps are not necessary to be done manually by the operator as they could also be automated by a computer by simply putting the necessary information. At first, after the exact location of the reported incident has been determined, the location of the 3 closest cell towers, that form approximately an equilateral triangle around the location of the reported incident, would have to be located. The mobile telephone network is divided into different cells where a base station is located at the center of each cell. The purpose of the base station, when necessary, is to send out a signal to a great number of receivers or even receive one. In general, it can send many signals at the same time as well as receive many signals from different users. After the base stations of these cell towers have been located, a triangulation could be performed in order to locate every phone number that is located in the area inside these 3 cell towers. Next, a list with all the numbers that are located inside this area would be created and be sent the warning message via Cell Broadcast. The way Cell Broadcast operates is by sending a message to multiple users in a geo-targeted and geo-fenced area at the same time. By following this method, not only individuals that are currently on that area will be notified about the fire incident but also individuals that happen to be passing through that area. This kind of method would be really effective in fire incidents reported in cities since there is a higher density of cell towers and base stations than on rural areas. In the instance of rural areas, the area of the triangle formed by the cell towers would be much bigger and by extent also the area of the triangulation, this does not mean though that the number of people that would receive the warning messages would be as high as the one in the instance of a densely populated city. The warning message that the



Emergency Warning

A user of the application Ignis Aiuto reported a fire related incident close to you. By tapping on the link below you can see the exact location of the incident on Google Maps.

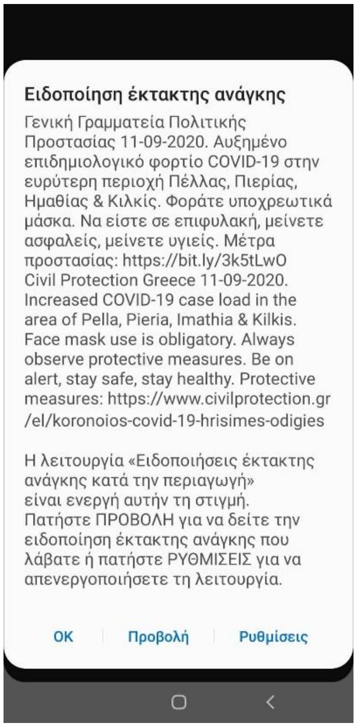
We suggest you get as far as possible from that location!

https://goo.gl/-maps/8VMgyT3x3wFEFxxMA

Figure 257 Warning Message that the people around the vicinity of the incident will receive

people around the vicinity of the event would receive is presented on Figure 17. As it can be seen, there is a brief message explaining what is going on as well as a Google Maps link which if the user clicks as he is asked to, he will see the exact location of the fire incident that was reported on the application of Google Maps, which is preinstalled on all the modern smartphone devices. After doing so, the user should get as far away as possible from that area. Last but not least, the operator(s) will contact the closest fire department and ask them to dispatch the necessary personnel in order to put out the fire.

So far, the operator's side when receiving a warning request and the steps he has to follow were explained in detail, in order to get a better view of this, it is worth mentioning an instance where a similar method was used in order to provide warnings to the general public by the Civil Protection Department and their bodies.



Ειδοποίηση έκτακτης ανάγκης

Γενική Γραμματεία Πολιτικής Προστασίας 11-09-2020. Αυξημένο επιδημιολογικό φορτίο COVID-19 στην ευρύτερη περιοχή Πέλλας, Πιερίας, Ημαθίας & Κιλκίς. Φοράτε υποχρεωτικά μάσκα. Να είστε σε επιφυλακή, μείνετε ασφαλείς, μείνετε υγιείς. Μέτρα προστασίας: https://bit.ly/3k5tLwO
Civil Protection Greece 11-09-2020. Increased COVID-19 case load in the area of Pella, Pieria, Imathia & Kilkis. Face mask use is obligatory. Always observe protective measures. Be on alert, stay safe, stay healthy. Protective measures: https://www.civilprotection.gr/el/koronoios-covid-19-hrisimes-odigies

Η λειτουργία «Ειδοποιήσεις έκτακτης ανάγκης κατά την περιαγωγή» είναι ενεργή αυτήν τη στιγμή. Πατήστε ΠΡΟΒΟΛΗ για να δείτε την ειδοποίηση έκτακτης ανάγκης που λάβατε ή πατήστε ΡΥΘΜΙΣΕΙΣ για να απενεργοποιήσετε τη λειτουργία.

Figure 248 Emergency Warning sent out by the Greek Civil Protection during the Covid-19 Pandemic (source: https://parallaximag.gr/epikairotita/minyma-112-politiki-prostasia-proeidopoiei-osous-einai-stin-pella-pieria-imathia-kai-kilkis)

During the COVID-19 pandemic in Greece, several emergency alerts were sent to specific geographic locations that had high number of cases, by the Civil Protection in order to warn and remind people about the measures they should be following. Those measures included the obligatory use of a face mask as well as maintaining a safety distance from one another. The message that was send to the areas of Pella, Pieria, Imathia and Kilkis on the 11th of September of 2020 can be seen on Figure 18. The message was written both in Greek and English. The method that was used on this instance is the same one that was presented above, through Cell Broadcast. The only requirement for Cell Broadcast to function properly on every smartphone device is to have the smartphone device updated to the latest operating system as well as set it to receive Cell Broadcast alerts (which is already activated by default in most of the newest smartphone devices. Another feature of this method, is the fact that when the population received this message the smartphone device made a characteristic unique sound and the phone vibrated for several seconds. Another measure that was taken during this emergency was with respect to the part of the population that did not own a smartphone device but rather a mobile phone, for this part of the population the Civil Protection of Greece sent out text messages (SMS). This element of example could also be adopted by the application that is being presented in this thesis. The combined population of these areas is roughly 450.000, no data could be found as to how long it took for the message to reach every person within these areas but according to parallaximag.gr, a local magazine and news site, the citizens received the emergency warning around 13:00 (2020).

Chapter 3: Legal and Ethical framework of Ignis Aiuto

3.1 Big companies, data breaches and privacy violations

Nowadays, it is really common that the news take advantage of data breaches and privacy violations. Smartphone applications that leave their users and their personal information exposed to the malicious intents of potential hackers through weak security protocols or protection systems can pose an enormous threat to the daily lives of users and even impact them negatively to an irreparable level. The extent of that damage, can range from the user having his email address leaked which could lead to have the email address bombarded with ads and promotions, to the theft of bank account information, or to having the entire digital identity stolen.

Someone would assume that such incidents would happen solely to small applications that have a background of inexperienced staff and developers or to companies that have been on smartphone application field only for a short period of time; on the contrary, companies such as Facebook, WhatsApp, Snapchat and Google have committed violations of data privacy. According to an article published by Forbes, an American business magazine, in September 2019, 533 million Facebook users' phone numbers and personal data were leaked online (Dellinger, 2021) after a data breach by hackers. As reported by The Guardian, a British daily newspaper (Associated Press in New York, 2021), among the leaked personal data, there were the full names of the users, their Facebook IDs, locations, birth dates, biographies and email addresses. The leak was first made available online by hackers in 2019 and was locked behind a paywall in an effort of benefiting economically by the leaked data. During 2021 the data resurfaced again for free this time in hacker forums, this meant that anyone with a basic knowledge of navigating the hacking forums could gain access to those data. This practically meant that anyone had free access to the data of more than 20% of Facebook' users at that time. Business Insider, an American financial and business news website, after conducting investigations later confirmed that those data that were included in the leak were indeed authentic and not false or fake (Holmes, 2021).

Another example of such exploitation of data is the flagrant Facebook-Cambridge Analytica scandal, where in accordance with The New York Times, an American daily newspaper, personal data of millions of Facebook users were collected by the British consulting firm Cambridge Analytica, without the consent of the users, substantially for political advertising (Confessore, 2018). As stated in an article of CNBC, a business and financial news network, Cambridge Analytica collected data through a smartphone application called "This Is Your Digital Life". The application, contained a series of questions that the user had to answer which would allow Cambridge Analytica to build the psychological profiles of its users. Along with this, the application would also collect the data of the users' Facebook friends via the Facebook's Open Graph platform without their consent (Meredith, 2018). On the same article, CNBC also states that, several days after the scandal came to light, Mark Zuckerberg, founder and CEO of Facebook, stated in a post on his personal Facebook page, the timeline of the event as well as all the measures that the social media platform has taken and will take from now on in order to avoid such incident ever happening again (Salinas, 2018). In accordance with an article published by the Business Insider, in the aftermath of what happened and after several lengthy trials, Facebook was penalized with a 5 billion dollar fine by the Federal Trade Commission (FTC) (Hamilton, 2019).

BBC, the British national news broadcasting corporation (2014), states that in 2013, Snap inc. the company behind Snapchat was warned about a vulnerability in Snapchat's application by an Australian security firm, Gibson Security. Snapchat did not respond to those warnings for 4 months and when they did it was already too late because hackers had already managed to exploit the vulnerability that was highlighted by the security firm. The hack had as a result the leak of the usernames and phone numbers of 4.6 million users. On another instance, as reported by Forbes (2021), a vulnerability on Whatsapp's application left exposed all 2 billions of its users to hackers. The exploit involved hackers hijacking the Whatsapp accounts of everyday users and blocking them entirely from their own accounts simply with the use of their phone number, the risk was enormous and it could impact millions of users that use Whatsapp as their primary communication tool. On another article, Forbes (2018) states that, between 2015 and March of 2018, outside developers were able to potentially access personal Google+ profile data due to a bug on the code. When the bug was discovered, Google decided to not notify the users of the social network in fears of having their reputation damaged which according to an internal memo could result into damages similar to the ones Facebook had when the Camebridge Analytica scandal came to light. According to a "detailed analysis" that Google ran, about 500.000 Google+ accounts were affected by the bug.

These incidents are some glaring examples of how easily people may have their privacy and personal information breached and violated without their consent and without having knowledge of how their data are being used. When a person trusts their data with a company, they should be sure that such essential information will not be mishandled or used for purposes other than the agreed ones. The protection of the user, his personal data and his identity, must be of utmost priority and be valued, respected and treated in a very transparent and serious manner rather than being used for money or personal gain.

3.2 Legal Framework

According to iubenda.com, an Italian based online service company that offers legal services to website owners, app developers, agencies and organizations, for an application to be covered on a legal level, there are certain criteria that should be met. These criteria have to be compliant with the domestic legal system as well as the European Union legal system, when it comes to companies that have their applications operating on the European territory. The design of the application that is being presented in this thesis will also follow the same guidelines. The criteria include:

- Privacy Policy
- Cookie Management
- Terms and Conditions
- Valid records of the consents the company collects
- Records of the processing activities
- Guides for services used by children
- Minors and General Data Protection Regulation

By taking all these into account, in the following section of the chapter all the problems that usually occur when it comes to smartphone applications and their users' privacy will be highlighted as well as how these issues could be avoided. Furthermore, it will be also discussed, how these aspects of privacy will be implemented in the design of the smartphone application that is being presented in this thesis, while always having the protection of the user's privacy as the top priority.

3.2.1 Privacy Policy

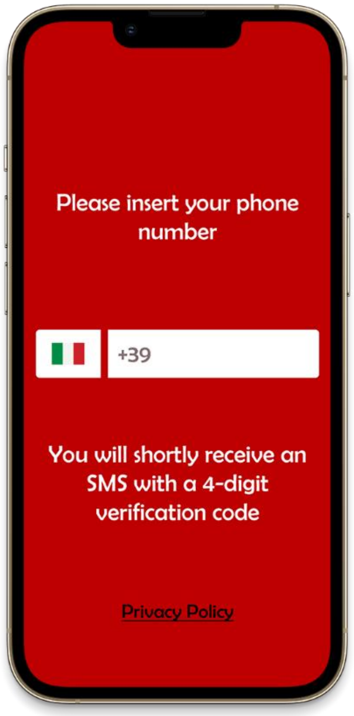
Before explaining the importance and use of privacy policy in smartphone applications, it is necessary to explain what privacy policy is in the first place. In accordance with Costante et al. (2012) privacy policy can be defined as the legal document which is used by a website or application, in order to communicate to its users how the personal data that are being collected will be managed. The privacy policy is a requirement for companies or developers who want to have their application featured on the Google Play Store and Apple App Store. This essentially means that if a company or a developer does not have a privacy policy for their application, then that application will not be accepted to become publicly available for downloading by smartphone users.

According to Balebako et al. (2014) after a survey that they conducted, where a number of smartphone application developers were interviewed regarding their knowledge about privacy policies, they found that privacy violations often happen due to the lack of understanding the privacy requirements from the developers' side rather than malicious intentions. Moreover, many of the developers stated that they did not have any kind of formal privacy and security training but instead any knowledge they might have had regarding privacy and security came from social networks, the internet or specialists such as lawyers, within their working environment. Furthermore, some of the interviewees were neither aware that guidelines developed by government agencies regarding the suggested privacy and security practices dedicated to developers existed nor had they read any such document during their careers.

The results of the mentioned survey showed that, usually developers and small companies either do not collect or store users' data at all or they collect only the necessary ones such as the log in credentials. Instead, third-parties such as Facebook that are used for payment authentications collected this kind of information. Work previously done by Book et al. (2013) and Lin (2013) show that these third-party advertising and analytical services have the permission to collect sensitive data. To add to this, the interviewees stated that usually these third-parties provide their information about their data collection policy in really lengthy and complicated formats, which on one hand covers those third-parties on a legal level, but on the other hand it indirectly aims to discourage the users or even the developers to read it, which was indeed the case for some of the interviewees (Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, Lorrie Faith Cranor, 2014).

With these being said, it is clear that many issues are created by simply the lack of proper training and awareness of smartphone application developers concerning privacy policies and data collections which as a result leaves the application users in the dark. A proper application therefore should first and foremost have someone that is responsible for the proper documentation while also constantly making sure that what is written in the privacy policy is exactly what should happen while the user is utilizing the application. Secondly, the privacy policy should be as clear as possible while being easy to find in the user interface rather than being in the fine print. Also, the data stored should be encrypted when they are transmitted to the server or cloud of the application and from there they should be encrypted again when they are stored in order to provide layers of protection to the user in case of data breaches. Last but not least, the data collection should be strictly limited to the gathering of only the necessary data that would aid the user to achieve his need when using the application (Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, Lorrie Faith Cranor, 2014).

In the case of the smartphone application that is being presented in this thesis, the privacy policy and the data collection would be really simple to understand and easy to locate within the application itself. Since the objective of the application is not the one of profiting from it, but rather the immediate mobilization and rescue of the user and people around the vicinity of him, the only data that will be collected and stored for security purposes will be the phone number of the user as well as the cell-based location of him which will be transmitted by the user's device. Additionally, as stated above, the data will be encrypted during the transmission as well as when they are stored with up to date encryption software, thus providing layers of security. Furthermore, no data will be shared with any third-parties but only with the application's server, which has as an ultimate objective the reassurance of the user that his data is kept safe.



Please insert your phone number

+39

You will shortly receive an SMS with a 4-digit verification code

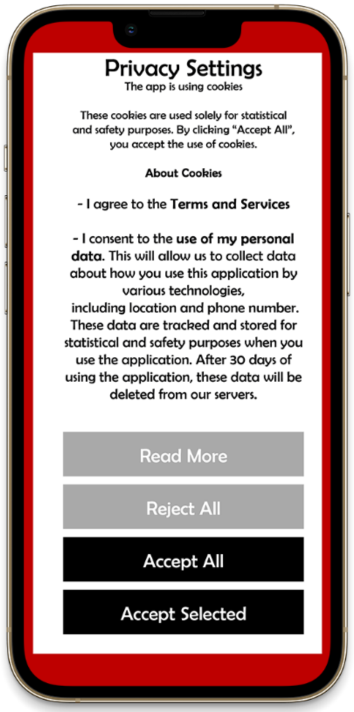
Figure 26 Privacy Policy Screen

3.2.2 Cookies Management

As stated in AllAboutCookies.com, a website that provides lots of information regarding cookies, their use and their purpose of existence; cookies are small encrypted text files which are usually used by developers to assist users to utilize and navigate a page or application efficiently. These cookies are stored always on the user's smartphone device or computer rather than on a server (All About Cookies). Cookies are primarily used in websites but their use is not limited just there, since the dawn of smartphones they have started appearing also on applications but their use is relatively restricted in comparison to desktop websites. According to SocialMediaToday.com, a news website regarding social media and technology, cookies on apps are used largely for the provision of ads to the user by tracking his online activity (Lele, 2014). In 2009 the European Union amended the directive that was passed on 2002, the ePrivacy Directive which came to be known as the "Cookie Law" due to fact that the directive was mainly dealing with the cookie consent and the data that was collected by companies and developers with its use (European Data Protection Supervisor, 2009).

It is obvious that when a tracker is attached to your online activity, security and privacy issues could occur. It is every user's right to be able to have his identity protected whenever he is using the internet. In accordance with AllAboutCookies.com, the way that ethical and responsible developers handle privacy issues that could occur by cookie tracking is done by clearly describing how cookies are deployed on their website. Another way that the cookies could be exploited, is when the user is connected to a non-secured WiFi network, this of course requires that someone intentionally tries specifically to steal that data by getting in between the connection of the user and the network itself. The chance of occurrence of such incident is really small but not zero.

With these in mind, it should be specified what would the policy of the application that is being presented in this thesis be when it comes to cookies and their use. First of all, the application will not be displaying any ads to the user which essentially means that the cookie usage would be extensively limited. That does not mean though that cookies will not be used at all, in order to be able to monitor and analyze the behavior of the users, some cookies will be stored. These cookies will store solely information along the lines of how many times was the application used for its intended purpose as well as how effective was the application. This could include the transmission times between the user's device and the cell tower as well as how fast was then the notification deployed to the individuals around the vicinity of the user. These cookies will be necessary in order for the application to function properly as well as to give feedback to the developer in case there are any functional issues with the application itself. Last but not least, the first time the user will open the application on his smartphone device, a small window will appear that informing him about the cookies that the application is using in a very clear and transparent manner. Then, the user will be prompted to accept them if he wants to continue using the application, because that will be the only way that the application will be able to get feedback about its use.



Privacy Settings

The app is using cookies

These cookies are used solely for statistical and safety purposes. By clicking "Accept All", you accept the use of cookies.

About Cookies

- I agree to the **Terms and Services**

- I consent to the **use of my personal data.** This will allow us to collect data about how you use this application by various technologies, including location and phone number. These data are tracked and stored for statistical and safety purposes when you use the application. After 30 days of using the application, these data will be deleted from our servers.

Figure 27 Privacy Settings and Cookies

3.2.3 Terms and Conditions

Terms and conditions describe the way that a smartphone application is intended to be used, this is done in order to protect the company or the developers behind the application from potential liabilities and, they usually contain information such as users’ rights as well as warnings and punishments about the misuse of the application. TermsFeed.com, an online company that provides legal agreements for online businesses such as websites and smartphone applications, states that there are five important reasons why it is necessary to have terms and conditions on an application (TermsFeed, 2020). Those reasons are:

- Prevent Abuse
- Terminate Accounts
- Own the Content
- Limit Liability
- Set the Government Law

It is of high importance to be as clear and as thorough as possible when writing these terms and conditions for the application that is being presented in this thesis in order to avoid any potential lawsuits that could ruin the trust that users could have for the application. By taking these important reasons about the terms and conditions into account, it should be considered how these reasons could be implemented in the terms and conditions of the application.

By taking into consideration the first two reasons, we can see that there is a direct correlation between these two. The first one sets the guidelines of how the application should be used in order for the user to have a smooth experience, while the latter is the result that abusive users could face if they do not use the application the way it is intended to be used. These aspects will be evidently and wholly elaborated on the section of the terms and conditions of the application.

A glaring issue that someone can notice with the way the application functions is that it is easily possible for someone to falsify the occurrence of a fire related incident. Such thing would create a lot of confusion and panic to the individuals around the vicinity of the user as well as it would alarm the authorities unnecessarily. In order to tackle this potential issue, we have to look on what the local legislation states for such malicious actions. On article 658 of the Italian criminal code with the title "Procurato allarme presso l'Autorità" which can be translated as "Alarm raised to the Authorities" it is stated that,

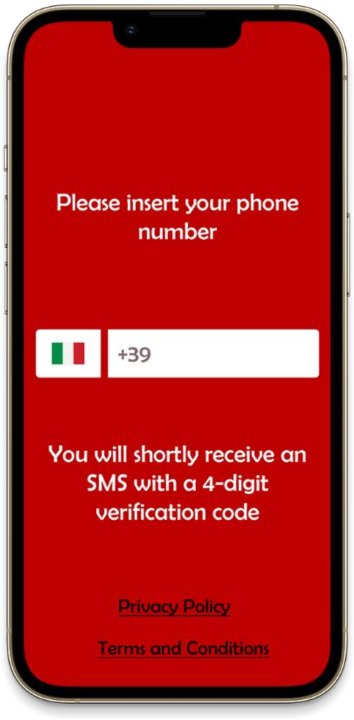
"*Chiunque, annunziando disastri, infortuni o pericoli inesistenti, suscita allarme presso l'Autorita', o presso enti o persone cheesercitano un pubblico servizio, e' punito con l'arresto fino a seimesi o con l'ammenda da euro 10 a euro 516.*"

This can be translated as,

"*Anyone who announces disasters, accidents or non-existent dangers, raises alarm to the Authorities, or the entities or individuals that exercise a public service, can be punished with up to 6 months of imprisonment or with a fine of €10 to €516.*"

The purpose of this law is to protect the authorities and more specifically their time and resources by not wasting them for unnecessary purposes but rather using them to stop crimes, put out fires and save lives.

Given the nature of the application in question, this law could pose as a warning in order to discourage users that may want to use the application for malicious intent. The way this warning could be implemented in the application is via a pop up before the user submits the request for the warning to be sent. After all, the user can be identified of who they might be because of the fact that nowadays the majority of the Europeans countries have implemented the Sim card registration law. The Sim card registration law states that, every Sim card has to be registered in order for it to be activated and consequently ready for use. For the registration the individual should have to use a valid identity document whether that is a passport or an ID card. This practically means that every phone number that is active and in use is connected to a physical entity.



Please insert your phone number

You will shortly receive an SMS with a 4-digit verification code

Figure 28 Terms and Conditions

3.2.4 Data Collected

Generally, companies behind smartphone applications tend to collect data of the user in order to create a user profile and then push targeted ads, products and services. Data collection and selling has become a huge business in the recent years since third party companies are willing to pay huge sums for said data. This of course, is a massive issue for the user since it usually happens without the knowledge or the consent of the individual, which as a result makes the user lose trust towards smartphone applications.

As mentioned earlier, the application that is being presented on this thesis, will not be collecting any form of data other than the necessary ones. The reason behind this decision is that it is vital for the user to be able to trust the application in order for it to be installed on his smartphone device and thus be effective. In accordance with Paljakka (2019), a study was performed where several users were asked about their behavior towards breached companies or companies that knowingly sell data to third parties. The result of this study showed that, individuals are less concerned when it comes to privacy issues when they trust a company or companies with a “good image”. This result can also be supported by Milne & Boza (2000) and Metzger (2004) who reported that having a relationship of trust between the consumer and the businesses reduces privacy concerns and plays a huge role towards the existence of these concerns.

To conclude, it should be disclosed what the policy will be behind the application that is being presented. The application will collect and store the phone number of the user as well as the location in case he uses the application to send a warning. This kind of data will not be sold or used in any other manner than the ones the user will agree to on the terms and conditions. The only reason that the phone number and the location of the user will be stored when the user uses the application, is in case the application is used for any malicious intent such as falsifying a fire related event. The data will be stored for 30 days for security purposes and then will be deleted. By collecting only the bare necessary data, it is ensured that a relationship of trust is built between the user and the application while maintaining a layer of protection towards the misuse of the application.

3.3 Ethical Framework

The Oxford dictionary defines ethics as “the moral principles that control or influence a person’s behavior”, in this instance it is obvious that the same definition can be applied for Ignis Aiuto. Generally setting an ethical framework for an application is not an easy task. The main issue lies with the fact that, there are no specific laws, rules or even code of ethics that a developer could follow in order to create a proper ethical framework for an application. Every aspect of the application has to rely entirely on the ethical compass that the developer has and given how easy it is today for developers to betray the users’ trust for money and personal gains, achieving such thing is harder than someone could imagine.

Furthermore, what is interesting about ethics, is that it is not something tangible, there is not a proper method or way to measure how much of an ethical person someone is, but rather it is something that should be seen through a black and white lens. A developer can either be deemed ethical or not, there is no in between, the concept of ethics is a fragile topic and should be treated with delicacy and transparency. The user should know from the beginning what he is signing up for, what is happening to his data, how his data are used and who has access to them, everything should be treated in a transparent manner.

Moreover, the primary target of Ignis Aiuto should be to gain the user's trust, we have to collect only the necessary data which would make the application run effectively while also creating a wide and lasting impact. The users' data should be treated the same manner as we would like our own data to be treated, we should ensure that we will collect only the data we would be comfortable sharing ourselves in case we were in their position. Money and personal gain should not the priority of Ignis Aiuto but rather improving the world by making the lives of our users and the people around them, safer one incident at a time.

Last but not least, we should also consider the nature of every application with respect its own ethical framework because not all applications serve the same purpose. For example, an application that tracks your running route and shows you the distance and duration of your run should not request access to anything other than your location. If it requests access to your contacts, camera or microphone for instance then something is wrong with the way that application is operating. Such application should not be trusted by the user no matter what the reason might be behind those requests, because more often than not, applications that operate in this manner do not have their users among their priorities but rather the user is viewed as a tool where the application and by extent the developer can profit off of him. As mentioned above, the data that will be collected from Ignis Aiuto will be limited to solely the necessary one that will have the application operate effectively and we will stand by this decision.

4. Conclusion

Throughout this thesis the design of a smartphone application that provides user generated emergency warnings for fire related incidents was discussed, an application that could potentially change the way people deal with fire related incidents on a local level. Smartphones are more popular than ever, more than 80% of the global population owns one, this number is expected to reach 91% by 2026, technology is at its peak and that should be the starting point for every country in order for such application to be implemented successfully. Creating an application that could potentially restructure the way we know emergency warnings could be hard, more often than not, new and revolutionizing ideas may take years to bring to life or may never even make it simply due to the lack of existing technology. This is not the case for Ignis Aiuto though, the fact that the technology already exists makes the whole process of realization plausible. The thing that Ignis Aiuto does, is to combine what already exists and builds on top of them. This has, as a result, the support from the average person that owns a smartphone, towards the government and local authorities of each country: using the application, it is possible to make a move so small, yet so powerful in today's world. If such application is used effectively, it could end up saving a lot of lives every time a fire related incident occurs.

References

All About Cookies. (n.d.). Welcome To All About Cookies.org. Retrieved from www.allaboutcookies.org: https://www.allaboutcookies.org/

Associated Press in New York. (2021, April 5). Facebook data leak: details from 533 million users found on website for hackers. Retrieved from The Guardian: https://www.theguardian.com/technology/2021/apr/03/500-million-facebook-users-website-hackers

Benoît Vivier, Chris Van Arum, Håkon Straume, Amélie Grangeat, Pablo Gómez. (2019, September 30). Public Warning Systems Version 3.0. Retrieved from European Emergency Number Association: https://eena.org/document/public-warning-systems-2019-update/

BRADLEY R. E. WRIGHT, AVSHALOM CASPI, TERRIE E. MOFFITT, RAY PATERNOSTER. (2004). Does The Perceived Risk Of Punishment Deter Criminally Prone Individuals? Rational Choice, Self-Cotrol, And Crime. JOURNAL OF RESEARCH IN CRIME AND DELINQUENCY, 180-213.

Centers for Disease Control and Prevention (U.S.). (2018). MMWR. Morbidity and mortality weekly report, Vol. 67, no. 30. Morbidity and Mortality Weekly Report (MMWR) , 829-832.

Centre for Public Impact. (2016, March 30). J-Alert: disaster warning technology in Japan. Retrieved from Centre for Public Impact: https://www.centreforpublicimpact.org/case-study/disaster-technology-japan

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. Retrieved from The New York Times: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Dellinger, A. (2021, April 3). Personal Data Of 533 Million Facebook Users Leaks Online. Retrieved from Forbes: https://www.forbes.com/sites/ajdellinger/2021/04/03/personal-date-of-533-million-facebook-users-leaks-online/?sh=58bc51b1717c

Doffman, Z. (2021, April 10). New Warning For WhatsApp Users Over Account Suspension 'Hack'. Retrieved from Forbes: https://www.forbes.com/sites/zakdoffman/2021/04/10/shock-new-warning-for-millions-of-whatsapp-users-on-apple-iphone-and-google-android-phones/?sh=1480f1287585

Dutch Ministry of Justice and Security. (2012, November 8). News: Nationwide launch of emergency alert system NL-Alert. Retrieved from Government of Netherlands: https://www.government.nl/latest/news/2012/11/08/nationwide-launch-of-emergency-alert-system-nl-alert

Dutch Ministry of Justice and Security. (2020, June 2). Documents: Factsheet NL-Alert Immediate information in an emergency situation. Retrieved from Government of the Netherlands: https://www.government.nl/documents/publications/2018/05/14/factsheet-nl-alert-immediate-information-in-an-emergency-situation

Dutch Ministry of Justice and Security. (2020, June 22). Nieuws: Ruim 90% van de Nederlanders ontving NL-Alert controlebericht op mobiel. Retrieved from Government of Netherlands:

https://www.rijksoverheid.nl/actueel/nieuws/2020/06/22/ruim-90-van-de-nederlanders-ontving-nl-alert-controlebericht-op-mobiel

Elisa Costante, Yuanhao Sun, Milan Petković, Jerry den Hartog. (2012). A machine learning solution to assess privacy policy completeness: (short paper). WPES '12: Proceedings of the 2012 ACM workshop on Privacy in the electronic society (pp. 91-96). Raleigh, North Carolina: Association for Computing Machinery. doi:https://doi.org/10.1145/2381966.2381979

European Data Protection Supervisor. (2009, June 6). Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XX0606(04)&from=EN

European Telecommunications Standards Institute. (2019, February 15). Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service. Retrieved from European Telecommunications Standards Institute: https://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.03.01_60/ts_102900v010301p.pdf

Fujinawa Yukio, Noda Yoichi. (2013, March 1). Japan’s Earthquake Early Warning System on 11 March 2011: Performance, Shortcomings, and Changes. Earthquake Spectra, pp. 341-368.

Fujinawa, Y., Rokugo, Y., Noda, Y., Mizui, Y., Kobayashi, M., and Mizutani, E. (2009). Development. Journal of Disaster Research 4, 218-228.

George R. Milne, María-Eugenia Boza. (2000). Trust and concern in consumers' perceptions of marketing information management practices. Journal of Direct Marketing, 5-24.

Hamilton, I. A. (2019, July 24). Facebook just got clobbered with a record $5 billion penalty over the Cambridge Analytica data breach. Retrieved from Business Insider: https://www.businessinsider.com/facebook-ftc-record-penalty-mark-zuckerberg-2019-5?r=US&IR=T

Herald Veenstra, J. Haverdings, Dirk van de Kamp, M. Nuver. (2012, December 14). Nieuws: Vuurzee bij kadowinkel in Tolbert (Video). Retrieved from 112Groningen.nl: https://112groningen.nl/Groningen/nieuws/20250/vuurzee-bij-kadowinkel-in-tolbert-video.html

Hilde. (2013, January 20). Nieuws: Grote brand in Meppel. Retrieved from RTV Drenthe: https://www.rtvdrenthe.nl/nieuws/70634/Grote-brand-in-Meppel

Holmes, A. (2021, April 3). 533 million Facebook users' phone numbers and personal data have been leaked online. Retrieved from Business Insider: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=US&IR=T

Lele, S. (2014, December 18). Cookies in Mobile: Do They Exist? Retrieved from www.socialmediatoday.com: https://www.socialmediatoday.com/content/cookies-mobile-do-they-exist

Lin, J. (2013, October 28). Understanding and Capturing People's Mobile App Privacy Preferences. Pittsburg, Pennsylvania.

Meguro, K., Fujinawa, Y., Kawakami, N., & Nishino, T. (2004). Impact of the earthquake early warning technology on society. Symposium on Earthquake Early Warning Application Systems, (pp. 53-59).

Meredith, S. (2018, April 18). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. Retrieved from CNBC: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic. Journal of Computer-Meditated Communication, 1-24.

Mitsuyuki Hoshiba, Kazuhiro Iwakiri, Yasuyuki Yamada, Naoki Hayashimoto, Toshihiro Shimoyama. (2011, May 22-27). Earthquake Early Warning and Observed Seismic Intensity. Retrieved from Japan Geoscience Union: http://www2.jpgu.org/meeting/2011/yokou/MIS036-P66.pdf

Motosaka, M., and Homma, M. (2009). Earthquake early warning system application for school. Journal of Disaster Research, 29-36.

News, B. (2014, January 2). Snapchat hack affects 4.6 million users. Retrieved from BBC: https://www.bbc.com/news/technology-25572661

O'Flaherty, K. (2018, October 9). Google+ Security Bug -- What Happened, Who Was Impacted And How To Delete Your Account. Retrieved from Forbes: https://www.forbes.com/sites/kateoflahertyuk/2018/10/09/google-plus-breach-what-happened-who-was-impacted-and-how-to-delete-your-account/?sh=63dbae366491

Paljakka, J. G. (2019). The Impact of Data Breaches on Cosumers' Attitudes and Behaviors. Vaasa: University of Vaasa.

parallaxi. (2020, September 11). Μήνυμα 112: Η Πολιτική Προστασία προειδοποιεί όσους είναι στην Πέλλα, Πιερία, Ημαθία και Κιλκίς. Retrieved from parallaxi: https://parallaximag.gr/epikairotita/minyma-112-politiki-prostasia-proeidopoiei-osous-einai-stin-pella-pieria-imathia-kai-kilkis

Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, Lorrie Faith Cranor. (2014). The Privacy and Security Behaviors of Smartphone App Developers. NDSS Symposium 2014. San Diego, California.

Salinas, S. (2018, March 21). Zuckerberg on Cambridge Analytica: 'We have a responsibility to protect your data, and if we can't then we don't deserve to serve you'. Retrieved from CNBC: https://www.cnbc.com/2018/03/21/zuckerberg-statement-on-cambridge-analytica.html

Smith, A. (2018, March 21). There's an open secret about Cambridge Analytica in the political world: It doesn't have the 'secret sauce' it claims. Retrieved from Business Insider: https://www.businessinsider.com/cambridge-analytica-facebook-scandal-trump-cruz-operatives-2018-3?r=US&IR=T

TermsFeed. (2020, December 18). Terms Feed. Retrieved from 5 Reasons Why You Need Terms and Conditions: https://www.termsfeed.com/blog/5-reasons-need-terms-conditions/

Theodore Book, Adam Pridgen, Dan S. Wallach. (2013). Longitudinal Analysis of Android Ad Library Permissions. Mobile Security Technologies.

Wong, S., Shaheen, S., & Walker, J. (2018). Understanding Evacuee Behavior: A Case Study of Hurricane Irma. UC Berkeley: Transportation Sustainability Research Center.

Wong, S., Shaheen, S., & Walker, J. (2018, December 1). Understanding Evacuee Behavior: A Case Study of Hurricane Irma. Berkeley: UC Berkeley: Transportation Sustainability Research Center. doi:DOI: 10.7922/G2FJ2F00

Yukio Fujinawa, Yoichi Nodab. (2013, March 1). Japan's Earthquake Early Warning System on 11 March 2011: Performance, Shortcomings, and Changes. Earthquake Spectra, pp. 341-368.