Marie Skłodowska-Curie Actions (MSCA)

Research and Innovation Staff Exchange (RISE)

H2020-MSCA-RISE-2017

Intelligence-Driven Urban Internet-of-Things Ecosystems for Circular, SAfe and IncLusive Smart CITIES

D4.1: IDEAL-CITIES Platform requirements and Architecture

Abstract: This deliverable describes the functional and non-functional requirements for the two pilot scenarios that will demonstrate and validate the IDEAL-CITIES platform, a discussion about circularity, resilience, and security requirements for the platform, as well as a presentation of the overall architectural design.

Contractual Date of Delivery	31/03/2022
Actual Date of Delivery	31/03/2022
Deliverable Security Class	Public
Editor	Konstantinos Vogklis
Contributors	NPS, BU, BLS, FORTH, DGS, ENPC
Reviewers	DGS, ENPC

The *IDEAL-CITIES* consortium consists of:

FOUNDATION FOR RESEARCH AND TECHNOLOGY -HELLAS	FORTH	GR
ECOLE NATIONALE DES PONTS ET CHAUSSEES	ENPC	FR
BOURNEMOUTH UNIVERSITY	BU	UK
BLUESOFT SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA	BLS	PL
DGS SPA	DGS	IT
NODAL POINT SYSTEMS	NPS	GR

This project is supported by the European Commission under the Horizon 2020 Program (2014-2020) with Grant agreement no: 778229

Table of Contents

1 Introduction and overview

This document outlines the requirements and architecture required for the IDEAL-CITIES Project platform. The purpose of the document is to allow the reader to identify the scenario requirements based around stakeholder requirements, assist the movement of the visually and mobility impaired and increase citizen safety through lifelogging.

This document relates to WP2 which identifies the multi-disciplinary factors affecting human perceptions of security of the IDEAL-CITIES Platform through user, trust and reputation models as well as risk analysis and perceived security requirements. WP3 is integrated within this document which provides the technical aspects under the infrastructure, monitoring, and adaption requirements. Lastly, the two pilots described within this document are related to WP5.

1.1 IDEAL-CITIES approach

The purpose of the IDEAL-CITIES project is to provide a platform to integrate IoT and IoTPS devices within a smart city context and facilitate developers to leverage these devices to create applications. This document approaches this endeavour in a top-down fashion, i.e. first the two actual applications are described to convey to the reader a real scenario of the platform's capabilities from an end-user perspective.

Following, from the end-user angle, the document continues with non-functional requirements which ensure that all applications and the platform operation per se, abide to the guiding principles of IDEAL-CITIES, namely circularity, resiliency, security and privacy. These principal requirements and how they will be achieved are described in detail. Furthermore, the requirements concerning the underlying platform infrastructure are detailed and summarized.

Finally, an overview of the IDEAL-CITIES architecture is provided, where all requirements mentioned above are grouped into logical entities, integrated within an enabling cloud infrastructure and allocated in the form of tasks to each partner. The document concludes with a summary of the requirements to be collected and the work to be performed.

2 Scenarios requirements

The scenarios will be based around the two pilots.

- Pilot 1: Assisting the movement of the visually and mobility impaired.
- Pilot 2: Increasing citizen safety through lifelogging.

In the following sections, each pilot will be described following the same structure:

- Scope and objectives of the use case
- Narrative of the use case
- Technical details
- Requirements

By following this methodology, the document aims to provide a comprehensive understanding of the requirements of the platform which will be submitted for testing, resilience and security.

2.1 Pilot 1: Fire evacuation scenario: Using location information to assist in a safe evacuation of citizens including visually and mobility impaired

2.1.1 Scope and objectives of the use case

The scope of the case will be geographically limited inside the Talbot House building of Bournemouth University (see Figure 1), nevertheless it could be easily extended to cover larger indoor areas like shopping malls and large venues. The IoT-enabled infrastructure will allow the IDEAL-CITIES platform to collect location information for all citizens inside the building.

The objective of the subject use case is to practically demonstrate how an IoTPS & smart city infrastructure can coordinate a fire evacuation plan using location awareness of citizens, on areas where GPS signal is either non-existent or noisy.

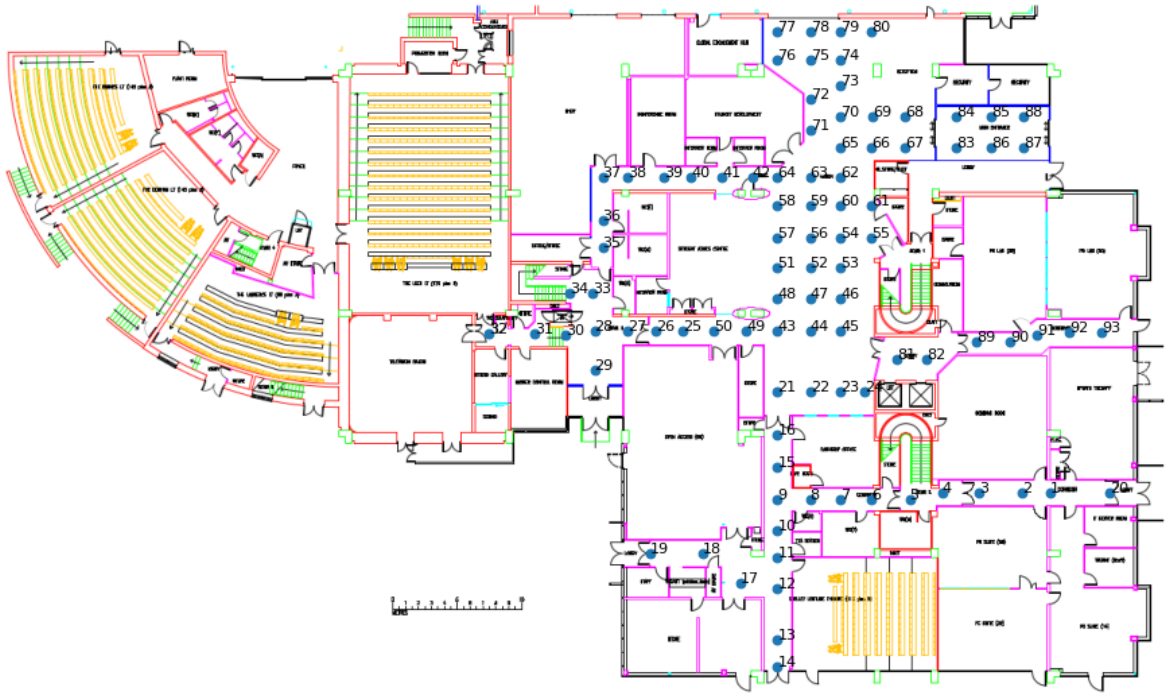

Figure 1 Poole House (Talbot campus) building floorplan (ground floor)

2.1.2 Narrative of the use case

In the emergency case of a fire evacuation scenario, one key challenge is to achieve continuous situational awareness of all citizens inside the premises and then navigate them to a safe environment. It is thus imperative to provide spatial information and navigation instructions to all citizens, including the visually impaired. Technologies for supporting navigation, including visually impaired persons, from a point A to a point B on a map. has been well defined and adequately solved. However, what is still missing, from current location awareness and navigation solutions, is knowing where things are and being able to decide the best path or what to avoid, i.e., steps towards a more general situational awareness. For example, in the case of an emergency fire evacuation some well-known exits may be blocked due to fire. The feedback of this information should be made available through communication channels and interfaces that will be appropriate for the level and type of disability of the user. The subject use case scenario focuses on a large-scale indoor environment, such as a university campus building, a museum or a mall, performing data analytics to extract a number of indicators of interest including an estimate of the indoor location and feeding them to the user in an appropriate manner.

2.1.3 Technical details

The pilot will involve one basic component which employs AI solutions (i.e. gradient boosted trees and convolutional neural networks) to compute the indoor location of the citizens.

This component is closely based on indoor location mechanisms for urban environment buildings without the use of GPS. The indoor location can be provided by using two mechanisms:

- Visual landmarks recognized by mobile device camera: This solution was initially proposed but has a serious limitation regarding the quality of the pictures taken in an emergency event. When in distress an individual may fail to direct the mobile camera to the selected visual landmarks. Landmarks could be:
  - well-known landmarks (e.g. a statue in a central place, a clock)
  - other signs suitably placed e.g. by the doors or on the floor to assist mobility
- Wi-Fi BSSIDs and signals of the nearby Wi-Fi networks: This solution was subsequently analysed and implemented because it only utilizes the signal from the nearby Wi-Fi antennas; no specific orientation of the mobile is needed and in general produces more accurate results.

A high-level description is as follows:

1st step – Acquiring building floor maps and models: A person carries a device comprised of a video camera, a storage module and a high-performance computing processor running appropriate software (this device could be a smartphone). When a person enters a specified building, the application automatically downloads from the cloud all the available information about that specific area, including a trained AI model that provided nearby Wi-Fi signals. An inside building location and a floor map will be displayed on the smartphone screen. The user is informed that all landmarks are "loaded" by an appropriate sonic notification. They can then proceed on their walking route and they can see on their screen the marker moving on the floor map. The tracking on the floor map will have the same semantics and feel similar to a GPS ride on a city map. It is worth noting that unless the user explicitly requests so, the IDEAL-CITIES platform is unaware of their location, since all calculations take place within the mobile device. The user can post their position to the IDEAL-CITIES platform at any time within the application interface.

Figure 2 presents the two-step procedure for acquiring the building's specifics and Figure 3 represents the indoor location components that operate within the user app.

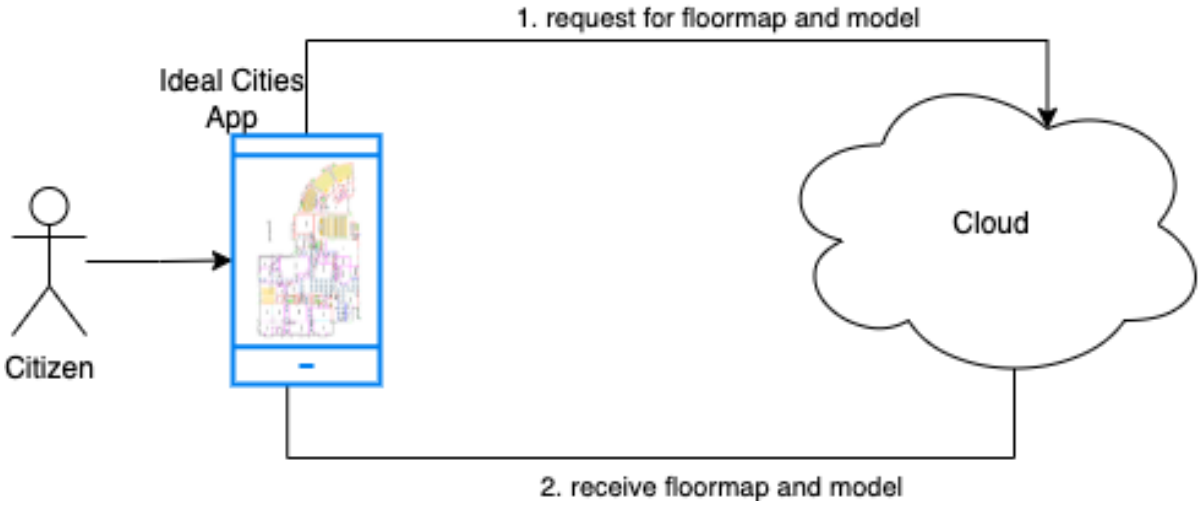

Figure 2 Download floorplan and location model from the cloud

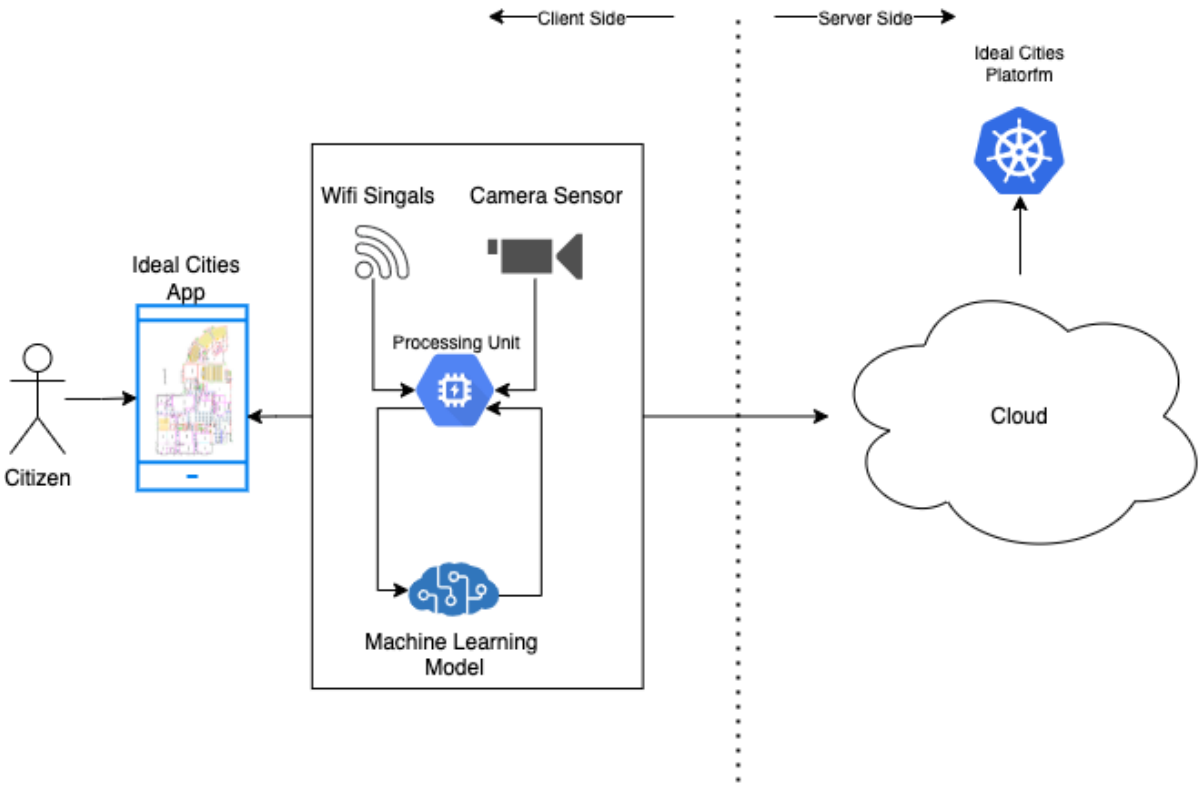

Figure 3 Continuous indoor position tracking using either Wi-Fi or visual landmarks. Client-side components live inside the App. The IDEAL-CITIES platform is only informed if the user allows it.

2nd step – Emergency fire evacuation: During the fire evacuation the IDEAL-CITIES platform can be used in either a supervised or unsupervised manner.

- Supervised operation: A general authority that monitors the building marks in real-time on the floorplan all the appropriate exits and all blocked exits (see Figure 4). This information is broadcasted to the people within the building.

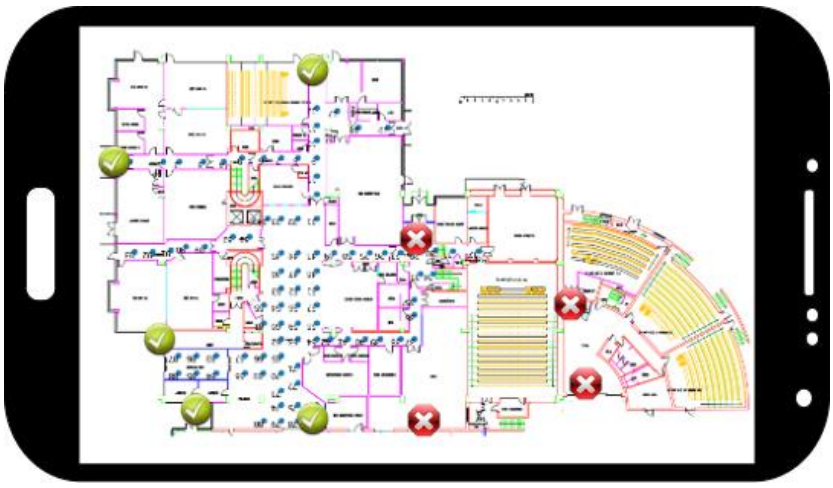

Figure 4 Marking available and blocked exits

Having this information available the user level application can now direct a user to the nearest exit. This information can be presented as a navigation route or in an augmented reality fashion (see Figure 5). For the visually impaired audio commands or appropriate haptics can be used to provide direction information. Further sensor-based information like accelerometers and magnetometers can be gathered to improve the location estimation and assess the stress level of the user. The users can also share images taken from mobile device cameras, so that the supervised authority can have a better overview of the situation.

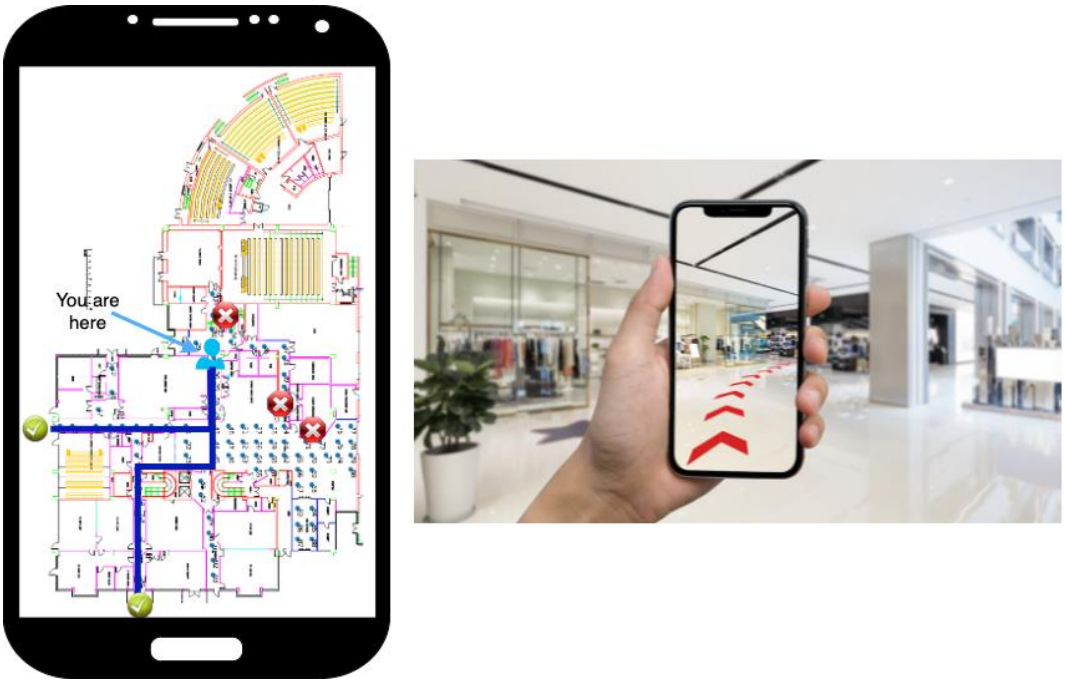

Figure 5 Evacuation information example

- Unsupervised operation: Using this operation mode no central authority is required; however, all users should publish their positions to the platform (see Figure 6). This way the IDEAL-CITIES application can detect the density of people or moving objects (see Figure 7) in a particular area and present this information to the users. The users can also share other sensor information or even images taken from the mobile devices.

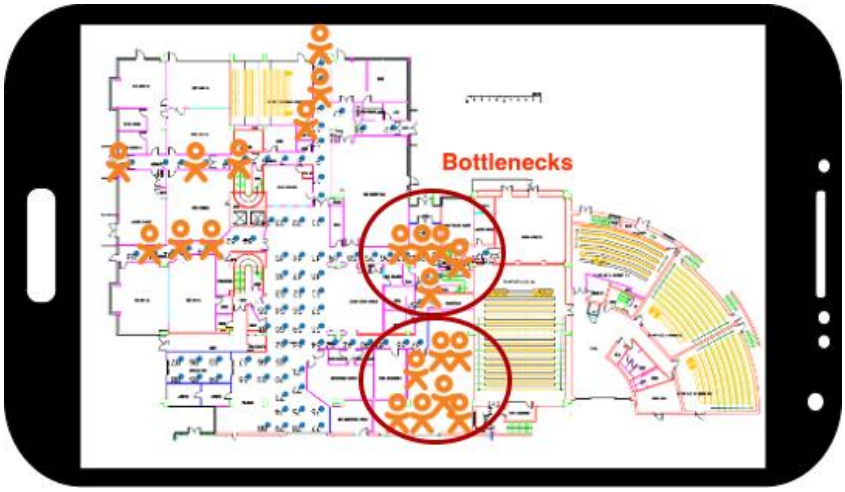

Figure 6 Unsupervised mode of App operation

Figure 7 Unsupervised mode heatmap of people density

2.1.4 Requirements

The requirements for Pilot 1 are as follows:

- IoT sensors (including smartphones) to collect the right data
- Wi-Fi receiver to collect nearby signals
- Cloud storage and databases
- Network technologies for transferring the data to and from the cloud
- Data analytics running on edge
- Special UI for visually impaired users

2.2 Pilot 2: Increasing citizen safety through lifelogging and location information

2.2.1 Scope and objectives of use case

Similarly, to Pilot 1 described in the previous section, the scope of this use case will be geographically limited; in this scenario we consider Bournemouth University's campus and a particular building (Poole House). However, the approach can be scaled for deployment in any large building i.e. mall, museum or any large area with poor GPS coverage.

The aim of this pilot is to increase citizens' safety and welfare by providing an easily accessible tool for lifelogging purposes. The goal of the tool is to practically demonstrate how an IoTPS & smart city infrastructure can be used as a lifelogging enabler, and by this, how it can positively affect citizen participation. At the same time attention is paid to, increasing responsiveness of the government and/or emergency services and improvement of citizen safety when facing a critical security and/or life-threatening situation.

Active lifelogging assumes the creation of a mobile application connected to a cloud platform that can monitor the indoor location of the user. Provided that all users consent in providing their locations and their specific role in the IDEAL-CITIES ecosystem, the application will be able to use this data to alert authorities or add to the data available to emergency services in the city. In addition, the user will have several options for the information submitted in the reports, including discreetly adding a photo or video to a report, providing more valuable data for public safety organizations.

2.2.2 Narrative of the use case

The narrative of this use case takes place inside the Talbot House building (Figure 1) of Bournemouth University but can be easily extended to any large indoor (or near indoor) area where GPS reception is poor. We assume the scenario that all actors have enabled the real time tracking from their lifelogging apps and the IDEAL-CITIES platform can record positions and roles. The role can be selected from some predefined emergency situations (e.g. first aid, medical doctor, law enforcement). Figure 8 presents the case where seven people allow the platform to track their positions.

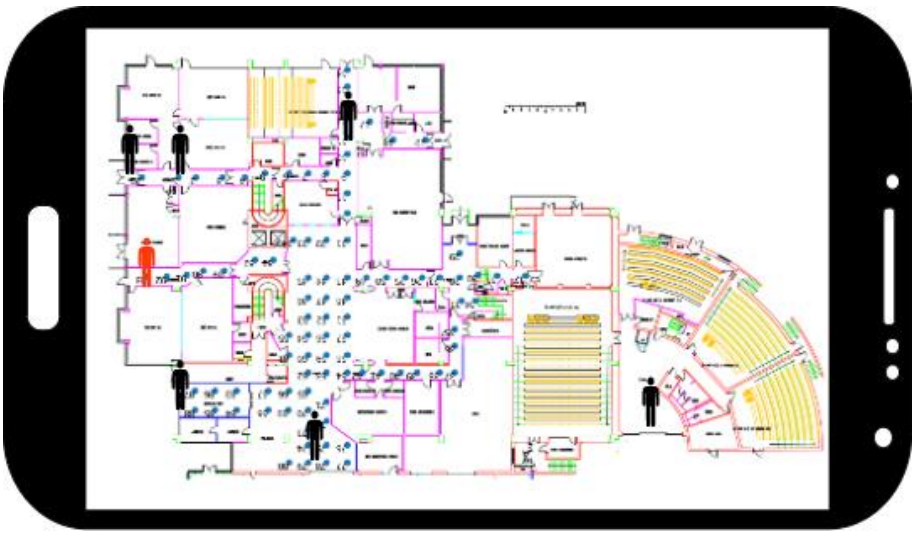

Figure 8 Assuming seven actors inside the building allowing indoor location tracking

The scenario then continues when one of the actors hits a “panic button” on their mobile application and raises an alert of some nature (medical issue, threat, etc.). The alert can be augmented with images taken automatically by the camera of the mobile phone and a set of recent inertial sensor data. The IDEAL-CITIES platform records the incident and performs two actions:

1. Reports the incident to public authorities.
2. Reports the incident to the citizens inside the building who have declared a corresponding role. The system can navigate the appropriate actors in real time to help the citizen in need. In Figure 9 we see a mock-up view from the IDEAL-CITIES application where the red-coloured actor raises a medical alert, and three other authorized actors are responding to the call. The IDEAL-CITIES platform broadcasts their indoor position and sensor data in real time, offering the shortest route to the incident.

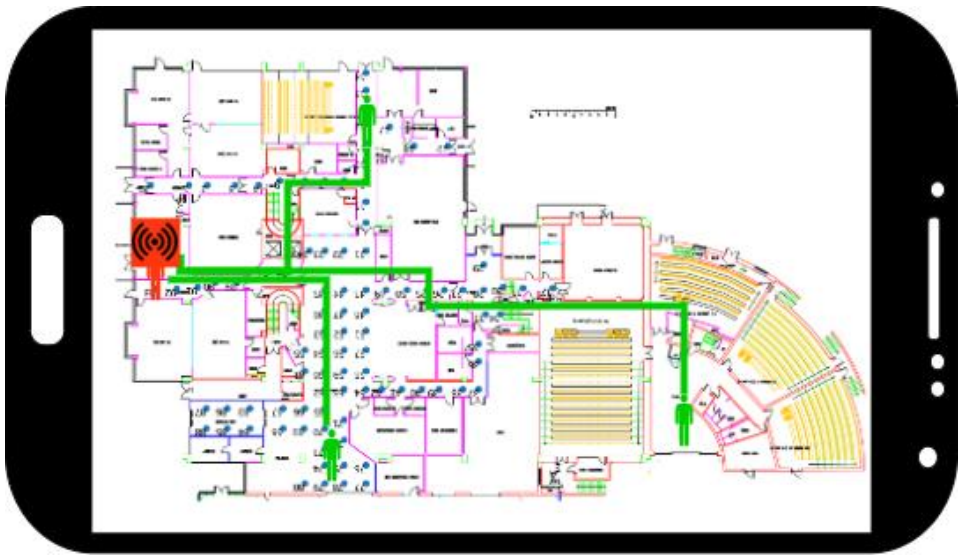

Figure 9 Alert is issued, and three corresponding actors have been informed

2.2.3 Technical details

The actors involved in the use case are:

- Citizens
- Emergency services which operate outside the IDEAL-CITIES scope

Lifelogging is a relatively new concept. It usually refers to ambient or passive data, but can also refer to the combination of data gained actively and passively (e.g. data gathered using wearable cameras and capturing real-world information accesses). In this scenario, we will focus on the passive lifelogging data, where an active report of the citizen can be enhanced by the actively collected data.

In this scenario, the data will come from the newly developed mobile application. This application will passively collect localization data, allow users to report an emergency, display the push notification, and ask for assistance (see Figure 10).

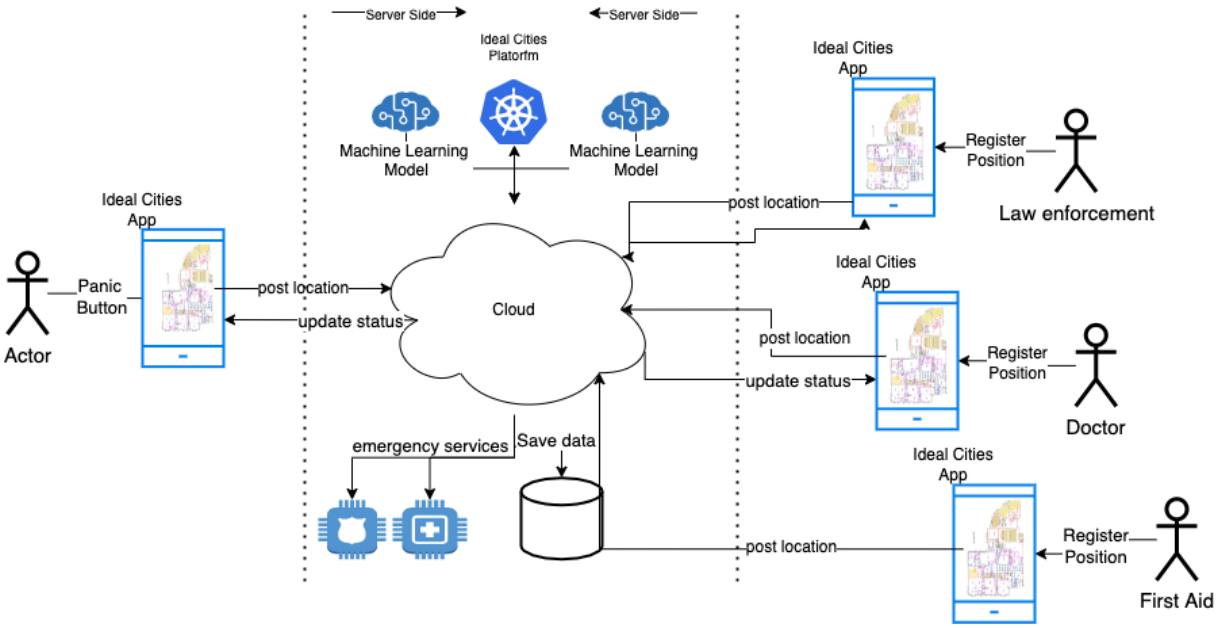

Figure 10 Flow driagram for lifelogging emergency

Data collected in such a way can later be reused and fetched by the city government to understand citizen needs and act upon on them.

Moreover, to enhance reports from users, the position of application users will be passively collected to alert them whenever they are close to the crime/law violation scene reported by other users.

2.2.4 Requirements

The data collected within this pilot will be analysed instantly or stored with intentions for further use (kept and used following the law and given permissions). A large amount of data should be analysed and/or collected in this scenario. There are specific challenges related to big data to be addressed, especially from the perspective of storage and data maintenance, organisation and retrieval such as semantic access, explore search, event segmentation, visualization of lifelogs, and lifelog annotation. Addressing these challenges will ease or make it possible to work with a vast amount of acquired data.

The requirements for Pilot 2 are:

- Smartphones
- Development of a smart application to enable active lifelogging within the application with dedicated UI
- Satisfy big data requirements from the perspective of storage, organization, maintenance, and retrieval
- Cloud/on-premises storage and databases
- Network technologies for transferring the data to and from the cloud
- Data analytics running on edge

3 Non-scenario requirements

This section will identify, analyse, cluster, and specify the requirements coming from technical WP3, the multi-disciplinary factors affecting human perception of security (WP2) and the pilots (WP5), factoring in distributed/cloud storage needs for the IoT sensor data, big data analytic capabilities, and the adoption of new clients/services. The requirements will also take into consideration circularity, resilience and security patterns as captured in deliverable D2.3.

3.1 Circularity, Resiliency & Security requirements

The adoption of a data driven circular economy paradigm, while it aims to address sustainability challenges, introduces significant privacy and security concerns. The need for continuous and seamless access to data in real time and the opportunities of adversaries potentially affecting the state of physical devices introduces high risks to both the physical and cyber plane. For the physical plane in particular, attacks against the confidentiality, integrity and/or availability of a device or data could lead to loss of human life. In this sense, resiliency refers to the ability of the system to recover from failures in a timely manner, ensuring business continuity.

In this section the circularity requirements following a document analysis exercise from WP2 are defined which in turn are treated as constraints that need to be satisfied even after the development and enforcement of security controls. As such, the elicitation and definition of security requirements considered the tradeoffs between circularity and security risks.

3.1.1 Circular Economy models – requirements

Throughout the Ideal Cities project the data-driven circular economy paradigm is adopted. This implies that circularity-by-design principles are followed both for the Ideal Cities platform as well as the data that are envisaged to be produced, consumed and reside in the Ideal Cities environment. In the following subsections requirements that explicitly enable or implicitly contribute to delivering data-driven circular economy are presented.

Location, Condition, and Availability

In the IDEAL-CITIES open platform, three attributes enable circularity: location, condition, and availability (LCA). The success of IDEAL-CITIES relies on the incorporation of an intelligent asset module displaying location, condition, and availability of all IoT devices. It should allow the monitoring of the device health and recommended maintenance actions. Manufacturing companies will then know in advance the product that they will receive, and the materials available for production [1] which will give them a competitive advantage regarding the development and the improvement of new products made circular by design.

Modularity, Scalability, and Functionality

The development of an open modular platform for building adaptive Internet of Things and Participatory Sensing (IoTPS) based smart city applications assisted with big data analytics and cloud services, that can improve quality of city life, by enabling citizens and authorities to produce and exchange contextualized information and alerts in real-time and in a trustworthy and sustainable manner.

The advocating of a modular design based on open standards is necessary to ensure:

1. the interoperability of the platform with existing IoT environments, big data analytics and cloud infrastructures, smart city services, networking, security and smart device technologies, and
2. the evolution of the platform, which is necessary to accommodate relevant technological changes and advancements in the future.

The use of open standards, standardized APIs and the principles of a modular, scalable, elastic, and multi-tier architecture in the design of the IDEAL-CITIES platform will ensure its ability to evolve and accommodate new developments in IoT, big data, cloud, and related technologies.

The modularity and the scalability of the platform will initially depend on the basic functional capabilities designed within the Logical Architecture, but further refinements are expected as a consequence of the experience gained from implementing the consecutive versions of the platform and the proof-of-concept IoTPS applications based on it.

The design and implementation of a distributed cloud backbone with scalable services to deal with the high influx of data will also need at the same time to provide the necessary degree of resilience from the perspective of handling security event and incident type of data. This is achieved by scaling up both the SIEM indexing services as well as the search heads, that is, the SIEM query interfaces and dashboards.

Unlike most value chains, the end-user of this kind of platform does not consume the data. The platform allows the use, reuse and repurposing of data, perhaps several times, at least until the data becomes out-dated. Even then it may become part of a historical trend which still has value.

End-to-end security/privacy dependability and operability

There are also the requirements for data collectors to protect the privacy and use of the data they collect (see for example General Data Protection Regulation GDPR[1]). Therefore anonymization, encryption, and authenticity preserving mechanisms will ensure sensitive information will not be available to any third parties without the user consent.

Adoption of new clients/services

The more people use a platform, the greater its utility and hence their value creation potential. Large platforms benefit from positive, self-reinforcing network effects, in addition to attracting producers, consumers and advertisers. The platform should provide mechanisms for end-users to provide feedback, with the purpose of improving services and enhancing its functionality.

[1] https://gdpr-info.eu/

3.1.2 User's trust and participation – requirements

From an information management and data governance perspective, smart cities are data and information processing infrastructures ingesting heterogeneous data from multiple sources (both human-to-machine and machine-to-machine) for use by a range of stakeholders and end users. At the same time, the data-driven circular economy paradigm mandates the promotion of sustainability through real-time decision making and optimisation. In practice, a smart city ecosystem that respects sustainability goals is envisaged as a system that is built upon concepts such as crowdsourcing and participatory sensing where the circular economy concepts are also applied to the data (such as reuse and repurposing of the data). In essence, citizens become *prosumers* – that is, producers and consumers of data and information. Furthermore, reflecting upon Wriston's Law[2] stating that 'capital', when freed to travel at the speed of light, will go where it is wanted, stay where it is 'well-treated', we could argue that in a data-driven CE ecosystem, capital is information and as such this will require a suitable architecture and stakeholder commitment to allow the data to travel and identify equilibria and locations where it is best utilised in order for such ecosystem to be viable.

It can be easily observed that trust would be of paramount importance in such a setting. Users/citizens would need to be confident that they will not live in a state of continuous and pervasive surveillance and that the privacy protection rules and laws will be upheld. GDPR would require that any smart city solution would inform the users on how their information is being processed and used. Although that this is a challenge in its own right, the expected introduction of AI in the very near future would exacerbate the problem. As such, the main requirements for promoting and supporting user's trust is transparency, traceability and explainability (in the case of an AI-enabled decision making).

3.1.3 Risk analysis and perceived security – requirements

The perception of security involves a multi-faceted, complex evaluation. In a smart city setting, perceptions can involve both safety (physical) and transaction related (cyber). Hence, perceived security in a smart city involves a new paradigm of citizen safety as the citizens will need to consider how they can protect themselves from both physical and cyber threats.

The data on physical safety in cities is widely available from a number of sources in the form of healthcare data (number of hospitals and respective healthcare system), crime rate, (such as terrorism and homicide rate) and so forth. Crime and related offenses data are also documented in higher granularity, such as robbery, car theft, burglary, kidnapping, vandalism, missing person, murder.

With regards to cyber incidents, as projected by many media outlets, they occur on virtually a daily basis. At the same time, cyber security education and awareness initiatives influence the intention of a citizen to engage in an online activity in a complex manner, as it can be both positive and negative; awareness is expected to shield and protect a user when performing online transactions but at it can also elevate anxiety. Smart cities are an interesting

[2] https://www.inspiringquotes.us/quotes/xLlu_AWq4w0Dz

environment as citizens may feel that they have limited choice in not engaging with online activities. As such, analysing the perceived security and risk is of high importance.

As such, perceptions on citizen privacy, especially in an environment of seamless and continuous data collection by a government or a local authority, seem to fuel the concerns on government's intrusion on personal life. A representative extended acceptance model for online transactions was conducted in [2] as shown in Figure 11 below.

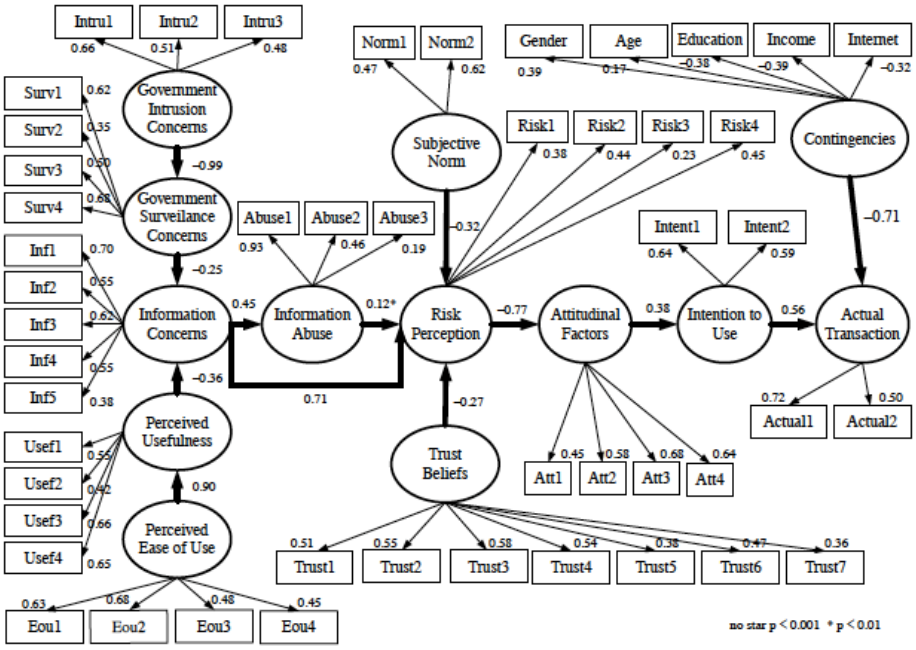

Figure 11 An integrated model for online transactions [2]

From the integrated model, the following behavioral aspects are noteworthy and relevant to IDEAL-CITIES:

- The indirect effect of government intrusion concerns on internet privacy concerns for information finding is significant (i.e. the relationship between government intrusion concerns and internet privacy concerns is "fully mediated" by government surveillance concerns [3]).
- The relationship between perceived ease of use and internet privacy concerns is fully mediated by perceived usefulness, that is, ICT is accepted to improve individuals' job effectiveness, performance and productivity.
- Risk perception is the major mediation variable between variables that increase risk (information abuse) and variables that decrease risk (trust, subjective norm), and the attitude of individuals toward using technology. With respect to individuals' attitudes toward using technology it has been found that this construct is a good predictor of intention to use the internet for online transactions, according to the theories of reasoned action and planned behavior [4].
- Unsurprisingly, age and gender does affect the intention to perform an actual transaction, with males of a younger age being more inclined to perform a transaction.

It should be noted however, that the research presented above was conducted prior to the introduction and enforcement of GDPR and as such the intention to perform online transactions to date may be stronger; however, since the attack surface of a city has considerably increased by enabling attack vectors comprised of both physical and cyber sources, the stronger correlation may eventually not be evident.

The increased smart city attack surface can be realized by observing the differences between conventional crime and cybercrime (see Figure 12).

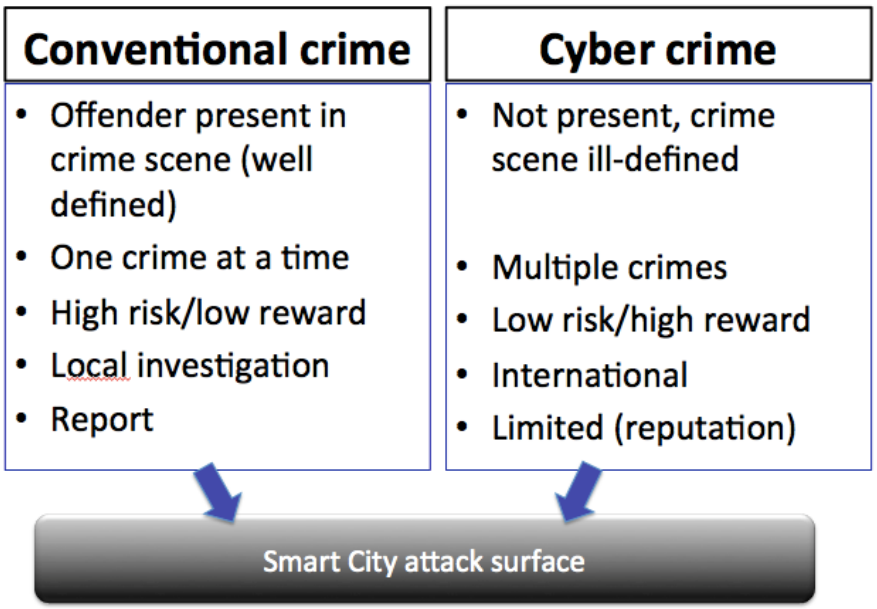

Figure 12 An increased attack surface for smart cities

Nowadays, cities become bigger and bigger every day. It is estimated that the urban population, which lives in big cities will almost double by the middle of the 21st century. The urban population will be 6.4 billion in 2050, as opposed to 2009, when the population was 3.4 billion. This rapid growth creates many challenges regarding the density of people in big urban environments. These challenges are related to pressures posed on care services (not enough carers), transport means (extensive traffic jams caused by the continuous increase of vehicles), urban population, healthcare (adequate centralised healthcare resources), citizens' safety (concerning both the physical and cyber planes), energy, industries and the economy in general. Especially, in the cases of people with disabilities who struggle with everyday life in an urban environment, the challenges are more demanding. Consider for example a visually impaired person having to navigate in a densely populated area, with limited contextual feeds (e.g. a riot or other hostile events evolving at a close proximity radius of them), or even trying to find a public seating space to rest. In order for all these challenges to be addressed, we believe that the usage of technology is necessary. The combination of technology and active citizens can be the key solution to the challenges that a big city should face. Citizens have the ability and potential to be active participants through technological enablers such as their smart phones. Smart devices are equipped with multiple sensors (e.g. cameras, GPS, and motions sensors) that are able to collect, exchange and report useful data regarding the situation in a city, like images, videos, audio, etc. Various kinds of technologies can be used in order to deliver these challenges, like big data analytics, cloud services and Internet of Things (IoT).

Smart city concepts have become one of the hottest technological topics during the last few years bringing and adopting innovative solutions and technologies like Internet of Things networks. Citizens can be connected among each other using their personal devices, like smart phones, laptops, and watches to exchange data; city services can inform other services and citizens regarding smart city infrastructure issues; the traffic can be handled using smart traffic lights and the drivers can be informed regarding the traffic around the city. All these services need data storage and exchanges to be successful. However, all technologies used are likely to have (software and/or hardware) vulnerabilities which can be potentially exploited by a threat actor, who may be interested to compromise the system and affect the smart grid.

Especially, IoT technology enhances the interaction between citizens and technology because the usage of smart devices like smart phones, sensors and objects of software applications creates new and diverse ways of capturing and processing information from various urban activities [5]. IoT networks include uniquely identifiable objects that can connect to the Internet and exchange data among each other without the help of human factors. Some of these objects are passive, which means that they simply scan and sense, and others are active and include microcontrollers and actuators. There are various kinds of objects, like security cameras, sensors, lighting systems, etc., that are connected between each other in smart way, using Internet network.

Even thought, IoT technology seems to be beneficial and helpful to smart city concepts, there are some barriers related to security, privacy and resilience that should be overcome. The security of IoT is highly variable, with some systems lacking encryption and security and privacy techniques. This fact makes these devices vulnerable to infections by malware and firmware modifications and of course open to hacking and other attacks. There are many use cases, where researchers have listed and performed various attacks over IoT network devices, such as hacking and denial of service (DoS) attacks.

Moreover, in IoT networks there are many nodes that do not trust each other. IoT networks are vulnerable to security attacks. In this way they can be compromised, a fact that has a significant impact on the operation, availability and performance of an application that is based on this technology. Furthermore, this kind of application handles and exchanges huge amounts of personal information of users, some of which may be sensitive. Vulnerabilities of IoT devices should be taken into serious consideration as this data concerns citizens and these devices exchange it. Compromising and gaining access over them, and the revealing of this data may have severe impact to citizens and smart city infrastructures.

The development of smart city platforms that are based on IoT technology and exchange personal data introduce a multitude of threats and risks that will need to be mitigated with appropriate security controls.

There are at least five threat categories in a smart city scenario. These categories are the following:

1. Threats on availability, which concern the unauthorised access to resources.
2. Threats on integrity, which include unauthorised changes of data such as manipulation and corruption of information.

3. Threats on confidentiality that include the disclosure of personal data by an unauthorised entity.
4. Threats on authentication, which refer to the access gained to stored data and services by an unauthorised user.
5. Treats on accountability, which is related to the denial of transmission or reception of a message by the corresponding entity.

Cyber security must address the vulnerabilities that will appear in order to protect the citizens and infrastructures of a smart city and prevent damages that can seriously affect the smart city environment. In addition, incident response mechanisms should be applied to detect intrusions on time and react faster.

For this reason, one of the biggest challenges that smart cities must take into consideration is related to cyber security. Cyber security is critical due to the potential of cyber breaches and incidents against critical sectors in a smart city. Some of the sectors that may be affected by breaches are shown in Table 1.

Table 1 Indicative threats and countermeasures on a smart city's assets and infrastructure

Sector	Threats	Countermeasures
Smart Buildings	• Infection by malware • System failure • Fraud by staff and unauthorized users • Controlling the fire system • Causing physical damage such as flooding • Disrupting building temperature (overheating or overcooling) • Damaging or controlling the lifts • Open windows and doors • Modifying smart meters • Opening parking gates • Disabling water and electricity supplies • Starting/stopping the irrigation water system • Stopping the renewable energy systems (RES)	• Two-factor authentication and one-time password for stronger authentication. • IoT forensics. • Threat and risk modeling • Data backup and recovery solutions to ensure reliability and continuity of services.
Transportation	• Sending false emergency messages • Disrupting vehicle's braking system • Stopping vehicle's engine • Triggering false displays in vehicle's dashboard • Disrupting vehicle's emergency response system • Changing GPS signals	• Public key infrastructure, digital certificates and data encryption solutions. • Misbehavior detection solutions • Pseudorandom identities.

Government	• Preventing of cybercrime • Identity theft • Disrupting critical infrastructure • Fiscal fraud • Altered files	• Data leakage prevention • Risk assessment • Insider threat analysis • Awareness training
Healthcare	• Modifying patients records or information • Exposing sensitive data unintentionally • Disrupting the monitoring system • Disrupting the emergency services • Sending false information • Jamming attacks • Sending an emergency alert • Eavesdropping sensitive information	• Secured Wi-Fi networks to guarantee safe handling of confidential information and personal data. • Risk assessment.
Energy	• Spoofing addresses and usernames • Unauthorized access and controls • Zero-day attacks • Botnets • Denial of service and distributed denial of service attacks	• Intrusion detection and prevention techniques. • Risk assessment. • Insider threat analysis. • Cybercrime intelligence.
Financial	• Loss of privacy • Accounting fraud • Disrupting business processes • Accessing confidential company information • Accessing confidential customer information • Damaging reputation • Defacing websites • Financial and reputation concerns due to fraud and data leakage • Denial and distributed denial of service attack • Phishing • Mobile banking exploitation • SQL injection • Malware (banking specific, Trojans)	• Anti-malware solutions. • Encrypted files and firewalling. • Fraud detection and prevention techniques. • Risk assessment. • Insurance to mitigate cybercrime risk. • Cybercrime intelligence.

Following the smart city maturity model introduced in D2.1, it can be argued that the higher a city's position on a maturity model is, the higher the expected impact of an exploit against a given vulnerability will be. By adopting a risk-based approach, we expect a vulnerability severity mapping to follow the layout shown in Figure 13.

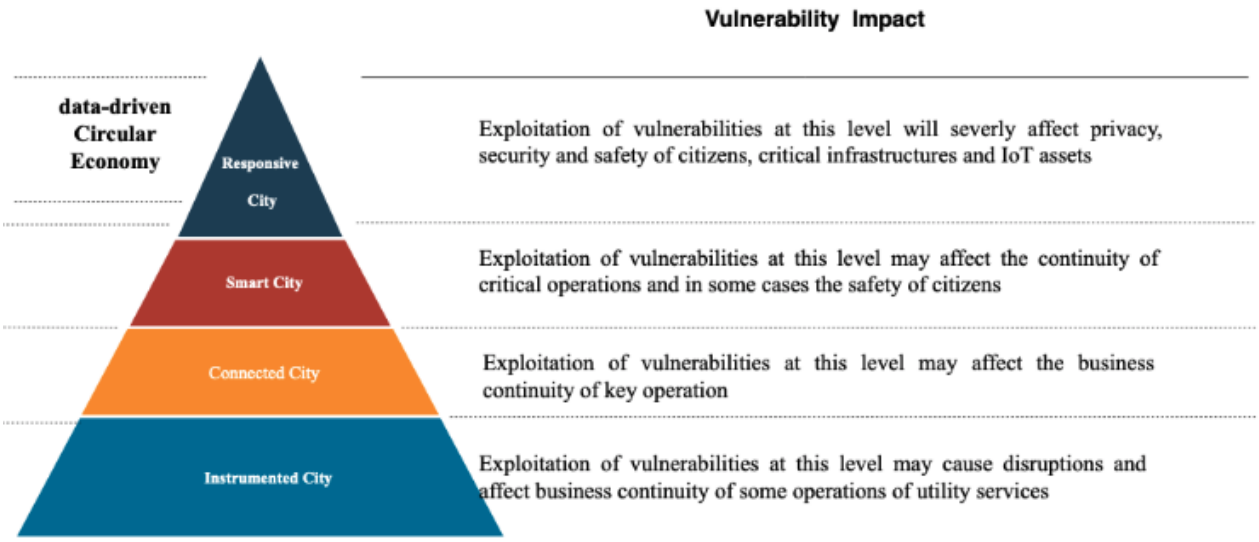

Figure 13 Vulnerability impact against the maturity level of a city (source [6])

According to our analysis conducted in [6], the impact of a vulnerability being exploited at a particular maturity level is expected to increase, as one traverses from a lower to a higher level. This suggests that a vulnerability will carry a larger amount of risk, the higher the maturity level this vulnerability will be placed on. More formally, if $R_m(\cdot)$ is some risk calculation function with m denoting the maturity level, then for a particular vulnerability v the following should hold:

$$R_i\,(v) \leq R_j\,(v)$$

for $i < j$. This means that if two cities have an identical vulnerability profile, the city with the highest maturity will also have the highest risk. This is captured in some quantitative vulnerability measurement systems such as the well-known Common Vulnerability Scoring System (CVSS), where the resulting severity of a vulnerability can be adjusted and subject to the so-called environmental variables. Furthermore, given a particular geographically confined space *c* (such as a country, a city or conurbation), we define the exposure of *c* as:

$$E_C = \sum_{u \in V_c} |v| * b_u$$

where V_c is the multiset of discovered vulnerabilities for *c* and b_u is the CVSS base score of vulnerability *u*.

Having defined the above metrics, one would be in a position to conduct an analysis based on the observed vulnerabilities from Open Source Intelligence (OSINT) tools such as Shodan [6]. By collecting geographically annotated device information, we correlate the observed, potentially vulnerability devices with the respective city's or country's metrics that describe the attainment of smartness. Indicative hypotheses tested, illustrating the security trends and perceptions are the following (as analysed and confirmed in [6]):

- H_1 The vulnerability exposure in cities increases with their population.
- H_2 The vulnerability exposure in cities decreases with their level of technology.

A noteworthy finding is that cities that have a high cultural score (such as universities in the top 500 list, international movement, but also number of theatres) revealed also a higher level of cybersecurity. This finding agrees with the position in [7] ”considering the way humans, government, and technology interact, security education is desirable to strengthen the knowledge of government officials and citizens with regard to cybersecurity issues”.

3.1.4 CRSP Patterns – requirements

As mentioned earlier in Section 3.1.1, data-driven circularity is comprised of three main properties, namely location, condition and availability. These properties are also viewed in conjunction with Resiliency, Security and Privacy as follows:

- **Location**: This refers to the physical, geographic location of the asset. This property should be defined for both mobile and fixed assets. In addition, the infrastructure should be **resilient**, by ensuring the availability of location services even when parts of the location capabilities are not functional; data repurposing and reuse (such as Wi-Fi SSID “noise” signal strength, visual markers, etc.) should allow the determination of location, accepting at the same time accuracy trade-offs (**data integrity**). In any case, the location data will still need to be correct and resistant against unauthorised modifications; historical data and crowdsourcing could contribute towards this goal. Location privacy can be offered by running the location services on the edge or mobile device and restrict any transmission of data to the cloud, unless the business logic dictates so (such as in case of emergency during a fire incident).
- **Condition:** The condition property is a declaration of the state of the asset in terms of its positioning in its lifecycle. An asset can be in good condition – which can be also further described by how close it is in its expiration date if applicable – requiring maintenance or service, refurbished, or recycled. Condition can contribute towards **safety**, by conducting predictions on when a device will likely become faulty and unusable.
- **Availability:** This property can describe three possible states: available, in-use, out-of-order.

In addition to the above primary CE properties, the following operational properties are also required:

- **Description:** Depending on the type of asset, the description will capture the respective characteristics that can be used to enable the circular use of the device. This is particularly relevant for constrained and specialised devices, such as IoT sensors, in which case the hardware profile will be captured. In the case of a physical asset, e.g. a parking space, its characteristics such as dimensions, capacity, etc. will be recorded.
- **Capability:** An asset can have more than one capability, as it can potentially serve many functions. An asset can have one primary capability which relates to its intended purpose and function, as well as additional capabilities. The primary capability will be the default use of the asset, e.g. a piece of land being part of a park, or a stretch of a street being a road for private vehicles. Additional capabilities would describe alternative uses of the asset; a park can become an overflow car park, whereas a street can be converted to a pedestrian’s access way.

3.1.5 IoT Cloud infrastructure and Big Data – requirements

This section is about the requirements to be implemented in the IDEAL-CITIES framework and architecture. It is anticipated that the IoT devices used to provide the services promised will require the use of sustainable cloud governance and big data systems.

As a starting point, the trust and reputation model, described in Section 3.1.3, explains the approach to ensure successful implementation and monitoring of all IoT devices with new client/services.

IoT and cloud computing represent two technologies that were originally very different from each other but which lately find more and more points of contact and application contexts that see them both involved. Transversely to these two technologies, the big data world is grafted, which, by its nature, finds important applications both in the cloud infrastructures and in the IoT field.

An IoT architecture is formed by small things (sensors, devices, etc) present in the real world characterized by limited storage and processing capacity. For the impact it can have on everyday citizen life, it represents one of the most disruptive technologies, empowering ubiquitous and pervasive computing scenarios. This deep presence in the maze of society and citizens' lives carries important consequential issues regarding reliability, performance, security, and privacy. On the other hand, cloud computing represents a well-established and much more mature paradigm which has virtually unlimited computing and storing capabilities with most of the IoT issues at least partially solved. The levels of reliability, security, data protection, performance provided today by cloud infrastructures allow their use applicable even to the most delicate and sensitive contexts.

In the context of IDEAL-CITIES, an IT paradigm in which cloud and IoT are two complementary technologies merged together is needed and it brings with it the need to better define the requirements that derive from the context of sensitive data and from the characteristics and degree of maturity of the adopted technologies.

Analysing the several mutual advantages deriving from their integration, on the one hand IoT can benefit from the virtually unlimited capabilities and resources of cloud to compensate for its technological constraints (e.g. storage, processing). Moreover, introducing the concept of big data analytics, fundamental in the context of IDEAL-CITIES, the cloud-based infrastructure provides a solution to effectively implement IoT service management and applications exploiting the data produced by them. On the other hand, the IoT represents an extension of the scope of the cloud architecture to deal with real world things in a distributed and dynamic way, together with the capability to deliver services in a large number of real-life scenarios, crucial for the IDEAL-CITIES project.

In an integrated environment, the cloud can be seen as an intermediate layer between "things" and applications, handling and partially hiding the complexity and the functionalities necessary for the implementation. The advantages of adopting this integrated paradigm can be classified in terms of:

- Computational resources: the limited processing capabilities of IoT devices that do not allow on-site data processing can be empowered by the cloud resource processing, also including the scalability which is challenging to achieve without a proper infrastructure.

- Storage resources: the huge amount of unstructured data produced by the IoT elements can be organized, classified, and stored in convenient and cost-effective solutions thanks to the data analytics capabilities of the cloud infrastructures.
- Communication resources: the effective and cheap solutions to connect anything from anywhere at any time through dedicated portals and built-in apps overcomes the IoT need of IP-enabled devices to communicate through dedicated hardware. On top of that a centralized management can monitor, control, and coordinate remote things.

Smart-city services must rely on a common middleware, able to acquire data from different heterogeneous sensing infrastructures and access different kinds of geo-location and IoT technologies, which can effectively expose information in a harmonized way. To create these platforms able to provision and support ubiquitous connectivity and real-time applications for smart cities, the following general requirements must be considered:

- 360-degree security: considering the kind of data managed and the ability to penetrate the territory and into everyday citizens' real lives, security is a key requirement and constraint. Not only at a technical level but also for the governance aspects (the team operating the platform must comply with industry-standard security controls).
- Reliability: there is a strong need for solid device connections since neither humans nor retry mechanisms are available on the "things" side.
- Scalability: the opportunity to add more and more devices until large amounts of elements must be possible and easily accessible. Moreover, the mechanism must be completely automatic with no need of adaptation of the underlaying architecture.
- Flexibility: the interface with applications and third-party tools is fundamental to extract information from data. The communication with these tools must be reliable and seamless to provide data analytics functionalities able to exploit the information from data and empower the IDEAL-CITIES platform functionalities.
- Simplicity: the user interfaces must be simple and intuitive, based on industry standard application interface for web developers. This allows administrators to change device configuration settings, automate processes, upgrade systems and firmware, and transfer files, on a schedule or when any kind of issue arise.

On the basis of these requirements, to meet the complex public sector needs, the resulting framework will consist of a sensor platform (with APIs for sensing and actuating) and a cloud platform for the automatic management, analysis, and control of big data from large-scale, real world devices.

3.1.6 Location mechanisms for indoor and urban environments – requirements

The location mechanisms for indoor and urban environments with poor GPS reception will be based on AI following two general paradigms (see Pilot 1 described above in Section 2.1):

a) Using mobile phone cameras to capture still images and apply deep learning methods (running on the edge) for detecting and identifying landmarks. Once landmarks are retrieved the position could be determined.
b) Using mobile phones to collect information about Wi-Fi antennas: SSIDs and signal strength, and feed this information into a machine learning model that will be trained

to map collections of SSIDs to specific locations (training via regression). This model can also run on the edge and can be more accurate than the landmark based one.

The requirements for providing location services are:

- Wi-Fi antenna to collect nearby Wi-Fi signals.
- Camera (possibly smartphone) for capturing the images of interest by the user.
- Algorithms for navigating indoor maps using start and end points.
- Cloud storage and databases.
- Network technologies for transferring data from the edge to the cloud and vice. versa, used to download the trained models on end user devices.
- Data analytics running on edge.
- UI for visually impaired users.

3.1.7 Security policy and mechanisms for security, privacy and trust – requirements

The IDEAL-CITIES platform should be underpinned by robust security and privacy policies. These security and privacy policies will be informed by leveraging existing expertise, policies, and processes in place within partnering organisations. Thus, a set of security and privacy policy requirements will be devised based on an analysis of each partner organisation's security and privacy policies. This will seek to identify first, common policy areas and then subject-specific policies that are likely to influence the trust, privacy or security of the platform and the services it delivers. From this, two overarching policies will be created, one covering security and one covering privacy.

3.1.7.1 *Policy Context*

As the IDEAL-CITIES platform is envisaged to be deployed in a smart city setting, the policies will define the roles and responsibilities of the relevant actors and key stakeholders. Against the above, the following policy components are relevant for a smart, circular city:

- On-boarding and off-boarding of organisations and data. As beneficiaries are expected to continuously join and leave the smart city infrastructure, there need to be clear on-boarding and off-boarding processes. When a new resource or application is offered to support or consume smart city functions, the application provider needs to specify the purpose of the application, data types needed, as well as any additional data generated.
- Incident handling processes. Capabilities for handling security and safety-related incidents as part of a holistic Cyber Physical Systems (CPS) approach will need to be defined. The transference of risk between the cyber plane to the physical plane will need to be addressed and escalation procedures for mitigating threats in both planes should be defined.

3.1.7.2 *Requirements*

This list of requirements will be organised in accordance with Volere principles[3]. This means that, for each requirement the following information will be captured:

1. ***ID:*** a unique ID will be created for each requirement.
2. ***Type:*** the requirements will be organised by type:
    a. ***Functional Requirements (FR)***: i.e. the essential or fundamental requirements that are necessary for the platform;
    b. ***Non-Functional Requirements (NFR):*** i.e. the behavioural characteristics that the specified functions must have these include:

        NF1. ***Look and feel Requirements***: i.e. style and appearance requirements.
        NF2. ***Usability Requirements***.
        NF3. ***Performance Requirements.***
        NF4. ***Operational Requirements.***
        NF5. ***Maintainability and Support Requirements.***
        NF6. ***Security & Privacy Requirements***: i.e. the security and privacy goals to be achieved, which for privacy will comply with the General Data Protection Regulation (GDPR) and be based on the privacy principles of GDPR (P1-7) and those in the Privacy Lifecycle PLAN (i-ix), that forms part of the Privacy and Compliance framework (PACT). These are:
            P1. ***Lawful basis for processing:*** the lawful basis for processing data will be specified, recorded and justified.
            P2. ***Purpose Limitation:*** personal data should only be processed for needed and specified purpose; no personal data should be reused without informed consent first being obtained.
            P3. ***Data Minimisation:*** only necessary data for the specified purpose will be processed.
            P4. ***Accuracy:*** the data will be accurate and kept up to date.
            P5. ***Storage Limitation:*** data will be pseudonymised or anonymised as soon as practicable and kept for no longer than absolutely necessary ('the data life'). At the end of the data life, data will be securely deleted and/or destroyed.
            P6. ***Integrity and Confidentiality:***
                i. ***Confidentiality:*** Ensuring data is only accessible to authorised stakeholders
                ii. ***Integrity:*** Ensuring non-repudiation and reliability for each piece of data, i.e. processing correct, authentic, and unmodified data.
                iii. ***Availability:*** Ensuring data is usable on demand and accessible to authorised stakeholders
                iv. ***Unlikability:*** Ensuring data cannot be sufficiently distinguished to linked across platforms or domains with similar context or purposes

[3] https://www.volere.org/

v. ***Unobservability/ Undetectability:*** Ensuring data is anonymised so that the anonymity and undetectability of the individual is preserved
vi. ***Anonymity:*** Obfuscating links between data and identity i.e. the ability to distinguish any one individual from the data
vii. ***Pseudonymity:*** Replacing identifying data with pseudonyms ensuring any links to original data cannot be made by unauthorised parties
viii. ***Intervenability:*** Enabling data subject access and/or supervisory authority access to affect action on the records (e.g. request modification and/or deletion). In that way it can be seen as a safeguarding measure that must be included within any process or system involving personal data
ix. ***Transparency:*** Openness - Providing assurance, accountability and traceability for internal and external stakeholders.

P7. ***Proportionality:*** Proportionality requires that any limitation on the rights of the individual have to be justified. For example, making sure that the measure(s) taken in processing the data do not disproportionally limit the rights of the individual whose data is being processed. A pre-condition is that the measure(s) taken in processing or safeguarding are sufficient to achieve the objective while only relevant personal data for the purposes of the processing is collected and processed.

NF7. ***Cultural and Political Requirements.***
NF8. ***Legal Requirements.***

3. ***Rationale:*** the rationale for each requirement will be noted.
4. ***Originator:*** a note of the user/document from which the requirement was derived will be captured;
5. ***Use Case:*** reference to the relevant use case (e.g. see Section 2 for pilot use cases) or, where these relate to other elements such as the platform design, a use case will be created for each requirement.
6. ***Fit criterion:*** testing the requirement for 'fitness' this shall include quality Metrics that measure and evaluate whether the requirement has been met i.e. the quality, function and suitability of the requirement.

For security and privacy (SP), the requirements will be described and organised under the following headers:

SPa. Access Requirements
SPb. Integrity Requirements
SPc. Privacy Requirements
SPd. Audit Requirements
SPe. Immunity Requirements

SPf. Legal Compliance Requirements

SPg. Standards Compliance Requirements

3.1.8 Software services and components monitoring – requirements

On every component and service that will be monitored, event captors will be created that will capture data and send them to the backend for processing. Those event captors will be of 2 types:

- Non-invasive: These types of captors will get data by parsing files that are generated by the software/component (e.g. log files). This way there is no need to alter the implementation of the monitored services/components.
- Invasive: Source code that IDEAL-CITIES will provide should be embedded into the source code of the respective service/component implementation to provide access to the data.

As aforementioned, on the backend, a service will be required to collect all those data from the captors to send them for analysis.

3.1.9 Adaptable infrastructure and Run-time adaptation – requirements

This section is strongly related to the use case requirements as technical requirements should always be based on the domain. In this particular example, those are the Internet of Things and smart cities.

The IDEAL-CITIES platform should be **flexible, extensible,** be able to easily adapt to **new clients, city services,** and emerging solutions (e.g. enhance the platform with new city monitoring services). The platform should also provide an easy way to plug new devices and smart sensors. The platform should also offer an **intuitive way to be accessible by citizens** and provide them with a way to interact with it to encourage people to use it.

The platform should be able to work in real time with a varying number of:

- Clients
- Services
- Devices

The smart applications created within the solution should **incorporate big data capabilities** to be able to analyse a vast amount of data in order to understand citizen interests and make it possible to **act upon them.**

Dockerize[4] an application

Applications should be designed to handle regular restarts and failures, changes in backend availability, and high loads without corrupting data or becoming unresponsive. Ultimately, they should be able to be scaled in a single image, which will allow the application to be scalable. Sample tools: Docker, Vagrant, Virtual Box.

[4] https://www.docker.com/

Container management

To ensure run-time adaptation, each component must be monitored, both in terms of resources (CPU, RAM, HDD) as well as user traffic. On this basis, the overseer application will be able to manage component resources. To manage IDEAL-CITIES containers, the use special tools for the deployment, maintenance, and scaling (Kubernetes, Apache Mesos) will be necessary.

Web of Things (WoT) Architecture

Interface standardization enables easy adaptation of new services. Therefore, it is important to define a common pattern by which communication will take place. The Web of Things (WoT) defines software architectural styles and programming patterns that allow real-world objects to be part of the World Wide Web. WoT assumes that the connectivity between the devices is achieved and focuses on how to build applications. By using WoT architecture it will be possible to easily adapt to new customers or services.

4 Requirements summary

This section summarizes the key requirements of distributed cloud storage systems, big data analytics capabilities, and adoption of new client's services.

The requirements summary can be divided into functional (scenario-based) and non-functional requirements.

4.1 Functional requirements

Both implemented scenarios include a mobile application that would operate as the user's access point to IDEAL-CITIES platform and the cloud-based IDEAL-CITIES platform. The mobile application is required to:

1. Authenticate the user, assign a specific role to them, and download the appropriate building model
2. Estimate the user's location using either Wi-Fi signals or visual landmarks from the camera.
3. Provide other inertial sensor data (e.g. accelerometer, magnetometer readings)
4. Navigate the use within the building when given two points on the floor map
5. Provide special notification mechanisms for the visually impaired

The IDEAL-CITIES platform is required to:

6. Provide user authentication
7. Provide administrative UI
    a. Management building model/floor map
    b. Record and view the user's position, sensor readings and/or images taken from their mobile phone camera
8. Broadcasting information to specific users in specific buildings
9. Inform external authorities about events
10. Secure all messages and transactions to enforce anonymity

4.2 Non-functional requirements

There are three major categories of non-scenario requirements namely: circularity, resiliency and security.

4.2.1 Circularity

In the IDEAL-CITIES open platform, three attributes enable circularity: location, condition, and availability (LCA). The success of IDEAL-CITIES project relies on the incorporation of an intelligent asset module displaying location, condition, and availability of all IoT devices. It should allow the monitoring of the device health and recommended maintenance actions.

4.2.2 Resiliency

Stakeholders will agree on the MTTR (mean time to recover) MTBF (mean time between failures) on the availability of the services. The core services (such as indoor location) will need

to be offered even when 30% of the underlying access points are unavailable. In a higher technology readiness level, geolocation will need to be further provided by the use of visual markers. Crowdsourcing and distributed computing approaches are preferred as they reduce the risks of single points of failure. In addition, crowdsourcing also supports the circular economy paradigm.

4.2.3 Security

The IDEAL-CITIES platform should be underpinned by robust security and privacy policies. These security and privacy policies will be informed by leveraging existing expertise, policies, and processes in place within partnering organisations. Thus, a set of security and privacy policy requirements will be devised based on an analysis of each partner organisation's security and privacy policies.

5 Architecture

This section describes the four architecture domains of the Ideal Cities platform. A focus is placed particularly on the component interactions that will come into play when implementing and evaluating the two use case scenarios (assisting mobility impaired and lifelogging).

5.1 Logical Areas – Components Functionalities

IDEAL-CITIES is an ambitious and extensive project, including many actors, points of view and use cases, incorporating multiple functions and processes, and aiming to satisfy a plethora of fundamental requirements. A high-level architectural breakdown of the areas to be addressed is as follows:

1. End-User Applications
    a. Smartphone App: This is the basic interface of the user and in its basic form can display the user's position within the building.
    b. Location Module: This component resides in the Smartphone App and repeatedly estimates the user's position within the building.
2. Platform Modules
    a. User Authentication & Management + APIs*:* This is an off-the-shelf module the provides auth2-compliant authentication services:
        i. *Normal Users*: The beneficiaries of the IDEAL-CITIES platform. They can have specific / predefined roles and be presented with the appropriate information.
        ii. *Administrators* (platform admins & developers): They import location models and floor maps and can gather information from and broadcast to all users within a specific building.
    b. Platform & Application Administration UI: This is the entry point for the administrators
        i. *Manage Location tracking models for each individual building*: Uploading location models and floor maps
        ii. *Specific UI to control all buildings*: The main dashboard where all the buildings can be monitored
    c. Applications & Application Management + IC HUB*:* The basic component of IDEAL-CITIES platform. All application logic must pass through this component.
    d. Asset Event Handling + APIs:
        i. Event Processing
            - Application-related events
                a) Assisted Mobility Engine
                b) Lifelogging Engine

ii. Event Dispatching

- Application-related events
  a) Assisted Mobility Engine
  b) Lifelogging Engine

3. Cloud Infrastructure
   a. Shared Storage
   b. Maintenance & Administration
4. Networking
   - Software Defined Networking Module

The interplay between the architectural areas from a logical perspective is depicted in Figure 14:

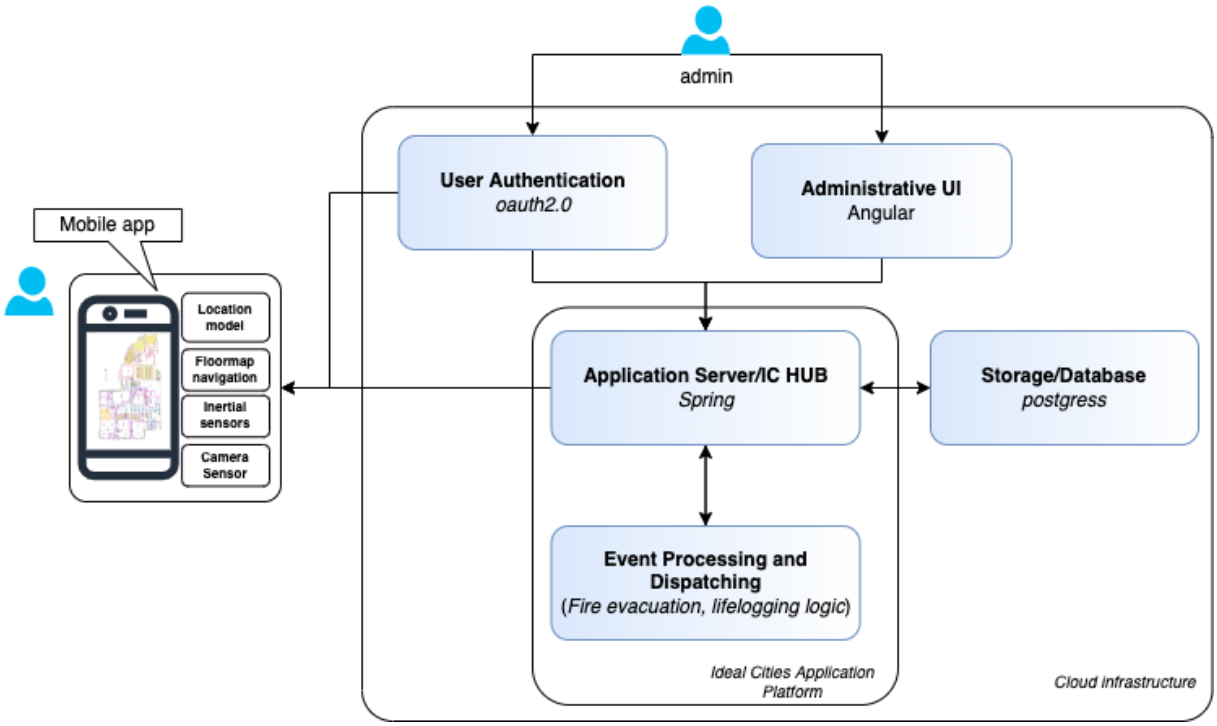

Figure 14 Logical Interplay of IDEAL-CITIES architectural areas

5.2 Architectural Approach

The multitude of the above areas necessitates a structured approach towards the architecture of the platform. Given the different angles from which the architecture can be viewed upon, it makes sense to use the common practice to divide the architecture into four domains, namely:

- Business Architecture: Identifies the business goals in line with the aims of the IDEAL-CITIES project and how they will be achieved in detail using Use Case Scenarios and Business Process Modelling.

- Application Architecture: Describes the required applications and their constituting components which enable the above Use Cases and Business Processes.
- Data Architecture: Describes the data model required for the applications to operate, as well as any interfaces between other applications internal or external to the platform
- Technology Architecture: The required logical and physical components which host the Application & Data Architectures and the required networking infrastructure.

The logical areas overarch these four domains. It is envisaged that logical areas will evolve into self-contained, functional modules which will be loosely coupled via the usage of standardized APIs and microservice-oriented architecture where possible. In this way, the extensibility, modularity, and scalability of the platform will be guaranteed.

5.3 Allocation of architectural tasks

The architectural elaboration and the actual implementation of the logical areas will be assigned to the partners as shown in Table 2:

Table 2 Implementation lead per IDEAL-CITIES partner

Architecture Task	Lead Partner	Contributing Partners
Mobile App	BLS	NP
User Authentication & Management	DGS	NP
Administrative UI	DGS	BLS
Application Server / IC-HUB	NP	FORTH
Event Processing and Dispatching	NP	ENPC
Backend Storage	NP	BU
Location Model	NP	BU

5.4 Sequence diagrams

This section presents some of the basic sequence diagrams that described the data flow for all the pilots. Starting with Figure 15 the basic login diagram is presented.

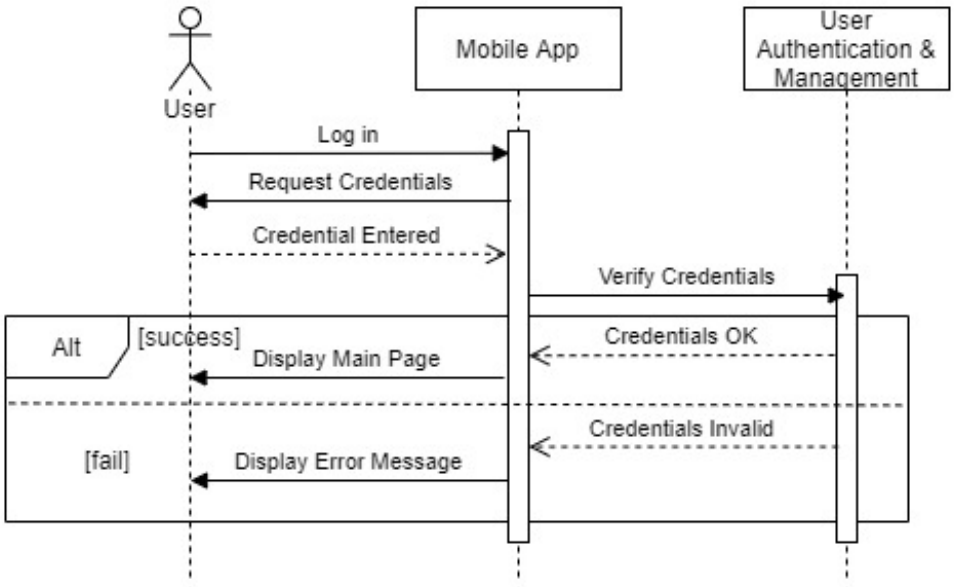

Figure 15 Login sequence diagram

The users get authenticated by the User Authentication and Management module and retrieve their personal profile details. In this step the IDEAL-CITIES platform assigns a specific role to each user. After a successful login the mobile app checks for an available GPS signal. When the user enters a known building then the mobile app downloads the corresponding map with the appropriate model, and switches to indoor location information. This is shown in Figure 16.

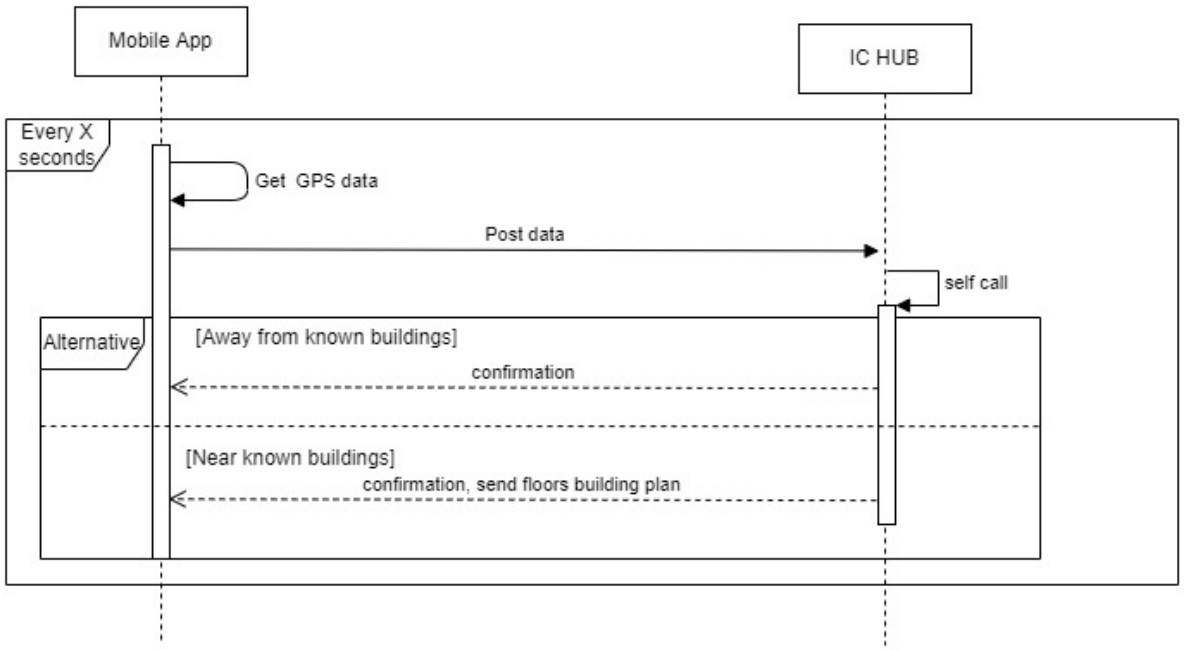

Figure 16 Mobile App checks for GPS coverage and switches to indoor location

The other basic sequence diagram it the one describing the continuous data flow between the IDEAL-CITIES app and the platform and is presented in Figure 17. There is a periodical data

exchange only if the user has allowed the IDEAL-CITIES platform to track his location and general situation.

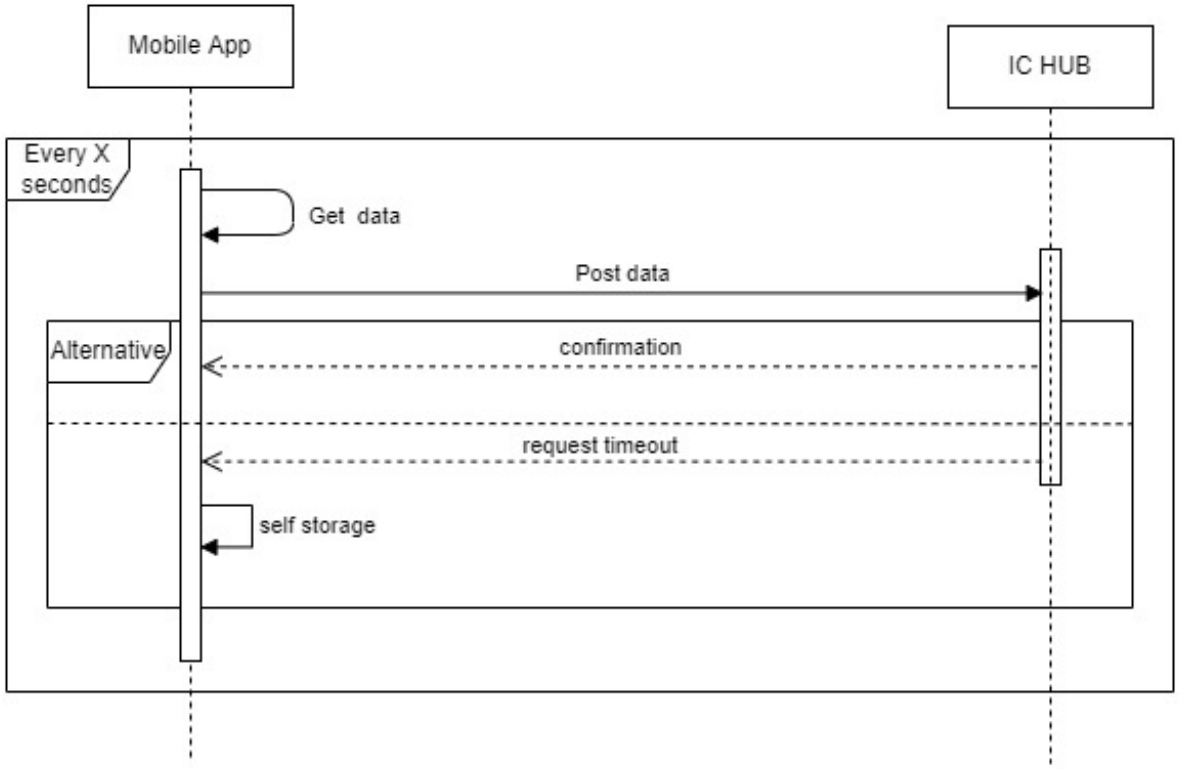

Figure 17 Data flow between mobile app and IDEAL-CITIES platform

The sequence diagram for the use case in Section 2.1 (Fire Evacuation) is presented in Figure 18. For convenience the diagram considers the actions after a successful login (see Figure 14). Most actions are performed in the IC HUB and the Event Processing and Dispatching modules. The most important message is the “push event of fire with evacuation plan” which is emitted towards the users from the Event Processing and Dispatching module. The evacuation logic is controlled form the Event Processing and Dispatching module using as input, among others, location data from the users via the IC HUB.

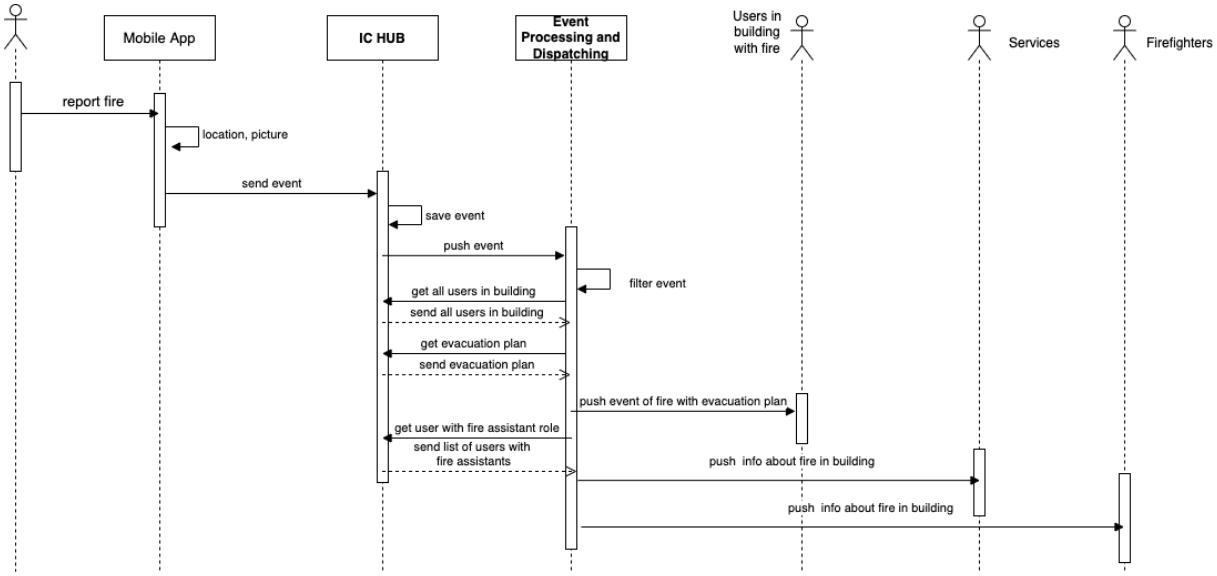

Figure 18 Fire Evacuation Sequence Diagram

The sequence diagram for the use case scenario of Section 2.2 (Lifelogging) is presented in Figure 19. Again, here, the login procedure has been omitted and it's assumed that a successful login was performed. According to the scenario the data flow begins with the request for assistance (panic button) from a registered user. The IC HUB receives alerting events and registers them to the Event Processing and Dispatching module. This module is responsible for filtering the alerts and forwarding them to the appropriate registered users (logged in with a specified role).

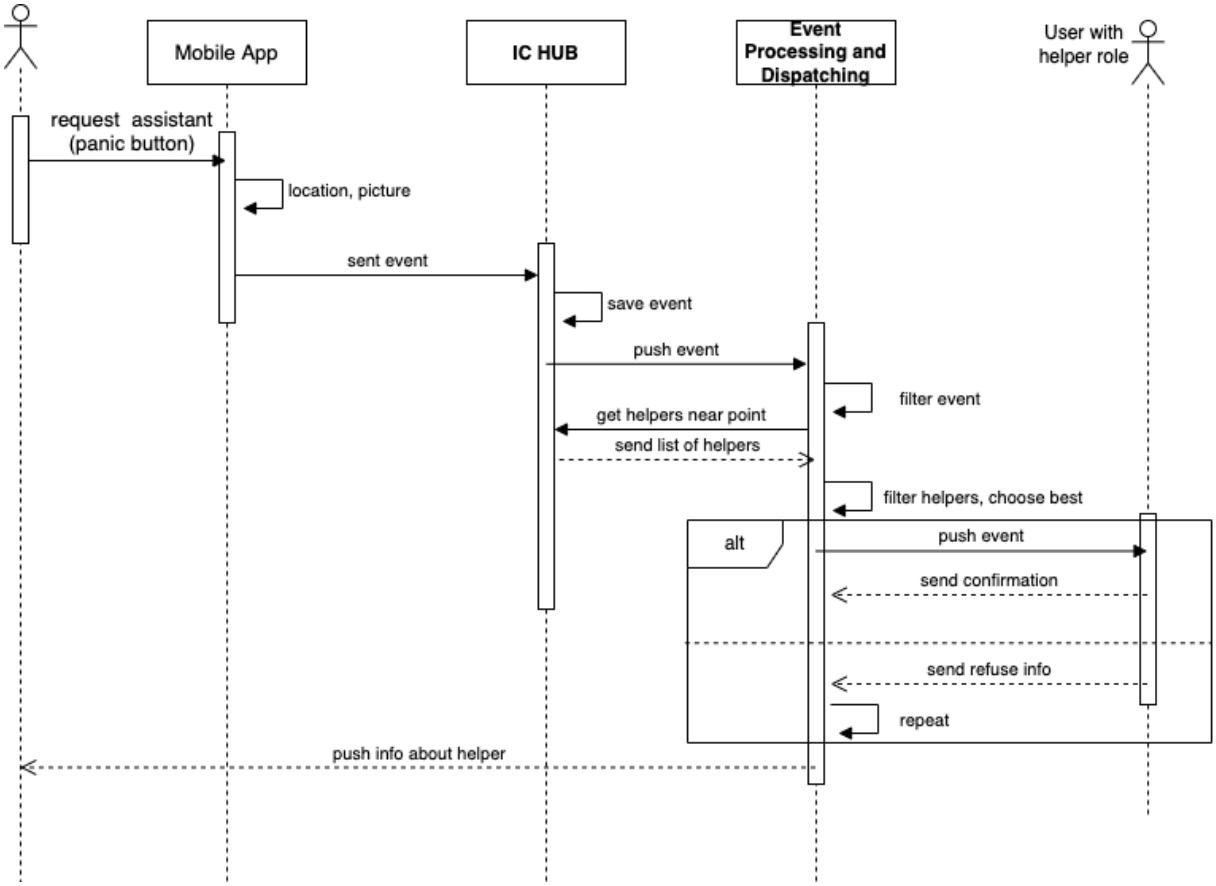

Figure 19 Citizen Safety through Lifelogging Scenario

5.5 API documentation

For the purpose of clarification and transparency, the OpenAPI Specification[5] will be used to create the API documentation in .yaml files

5.6 Repository

For this project, we have chosen GitLab as the official project software repository. The group IdealCities https://gitlab.com/idealcities has been created, where software projects for each platform component are stored.

[5] https://swagger.io/specification/

6 Conclusions

In regards to task T4.2, the platform architecture will gradually be refined using the approach described in Section 5.2, and by considering contributions from all partners, the overall reference architecture of the IDEAL-CITIES solution will be finalized.

Specifically:

- Using business use cases and business process models which overarch the logical areas described in Section 5.1, the APIs of the corresponding modules will be finalized.
- The input derived from the APIs will flow into the ongoing application design of the modules, thus enabling each partner to identify and specify any additional application components or enhance existing ones. At the same time, the data model of each module will be finalized, and data storage & sharing considerations can be formulated and designed.
- The technical architecture requirements of each module will be examined. They will flow into the integrated platform technical architecture, which will aim to reuse the required logical and physical components of the infrastructure where appropriate.

7 References

[1] Benjamin, G., May, B., Prema, M., Raghubanshi, V., (2019), “The coming evolution of field operations”, McKinsey & Company, available: https://www.mckinsey.com/business-functions/operations/our-insights/the-coming-evolution-of-field-operations [accessed 29 September 2019]

[2] Katos, V. (2012), "An integrated model for online transactions: illuminating the black box", *Information Management & Computer Security*, Vol. 20 No. 3, pp. 184-206. https://doi.org/10.1108/09685221211247299

[3] Baron, R.M. and Kenny, D.A. (1986), “The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations”, Journal of Personality and Social Psychology, Vol. 51, pp. 1173-82.

[4] Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), “User acceptance of information technology: toward a unified view”, MIS Quarterly, Vol. 27 No. 3, pp. 425-78.

[5] Monsivais, D., Ghosh, A., Bhattacharya, K., Dunbar, R. I., & Kaski, K. (2017). Tracking urban human activity from mobile phone calling patterns. PLoS computational biology, 13(11), e1005824.

[6] Paul-David Jarvis, Amalia Damianou, Cosmin Ciobanu, and Vasilis Katos (2021). Vulnerability Exposure Driven Intelligence in Smart, Circular Cities. ACM Digital Threats. https://doi.org/10.1145/3487059

[7] Zhen Li and Qi Liao (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. Government Information Quarterly 35, 1 (2018), 151–160. https://doi.org/10.1016/j.giq.2017.10.006

[8] Robertson, S., & Robertson, J. (2012). Mastering the requirements process: Getting requirements right. Addison-Wesley.