Multi-layered Security technologies to ensure hyper-connected smart cities with Blockchain, BigData, Cloud and IoT

White Paper

September 2020

Grant Agreement No. 814917

Multi-layered Security technologies to ensure hyper-connected smart cities with Blockchain, BigData, Cloud and IoT

Project acronym	M-Sec
Project Full Title	Multi-layered Security technologies to ensure hyper-connected smart cities with Blockchain, BigData, Cloud and IoT
Project Duration	39 Months (July 2018-September 2021)
Publication Date	September 7, 2020
Dissemination Level	Public
Contact	https://www.msecproject.eu/contact/

The M-Sec project is jointly funded by the European Union's Horizon 2020 research and innovation programme (contract No 814917) and by the Commissioned Research of National Institute of Information and Communications Technology (NICT), JAPAN (contract No. 19501).

Table of Contents

Glossary

AAA	Authentication, Accounting and Authorization
APPI	Act on the Protection of Personal Information
CIA	Confidentiality, Integrity and Availability
EU	European Union
FG	Functional Group
GDPR	General Data Protection Regulation
IDC	International Data Corporation
IoT	Internet of Things
IDS	Intrusion Detection System
JP	Japan
LDAP	Lightweight Directory Access Protocol
NICT	Institute of Information and Communications Technology
NIST	National Institute of Standards and Technology
SME	Small and Medium Enterprises
TCG	Trusted Computing Group
TPM	Trusted Platform Module
T&R	Trust and Reputation Model
UC	Use Case
ZB	Zettabytes

1. Introduction

This M-Sec white paper is a report that acts as a guide to inform readers concisely about the main IoT security issues faced nowadays and shows our philosophy and proposed solutions to these problems.

To do so, the report starts with an introduction of what is M-Sec about and what are the current challenges that the IoT market faces

Afterwards, on section 4, it is presented the methodology followed for building such a solution like M-Sec, including the procedure for the requirements elicitation. Once this was settled, the project as a whole worked on clarifying potential risks through the use cases analysis and requirements analysis. This labour resulted in the acquisition of a list of potential risks based on National Institute of Standards and Technology (NIST) standards and guidance, inviting to perform an exercise to categorize them and another one with the proposal of suggestions to proceed with their mitigation

Section 5, presents the set of solutions offered by M-Sec and following and end to end approach to ensure confidentiality, integrity, availability, and privacy on the whole cycle of the IoT ecosystem.

All in all, the sections of this white paper, conclusions in section 6 included, answer to this approach and readers might find how M-Sec deals with these topics and expects to solve the threats looming over its architecture.

2. What is M-Sec

M-Sec is an EU-Japan collaboration which stands for *"Multi-layered Security technologies to ensure hyperconnected smart cities with Blockchain, Big Data, Cloud and IoT"*.

The main goal of M-Sec project is to research, develop, deploy and demonstrate multi-layered Security technologies to ensure hyper connected smart cities and empower IoT stakeholders with an innovative platform which leverages blockchain, Big Data, Cloud and IoT security, upon which they can build innovative smart city applications.

This Research and Innovation action involving the cities of Santander in Spain (Europe) and Fujisawa in Kanagawa prefecture (Japan) started in July 2018 and will last until September 2021.

2.1 What does M-Sec do?

The project explores secure, interoperable interactions between IoT elements based on a holistic secured cloud/edge/IoT context within a future smart city. Overall, the M-Sec paradigm complements mainstream IoT/cloud technologies, through enabling the introduction and implementation of specific classes of applications and services, which are not efficiently supported by state-of-the-art architectures.

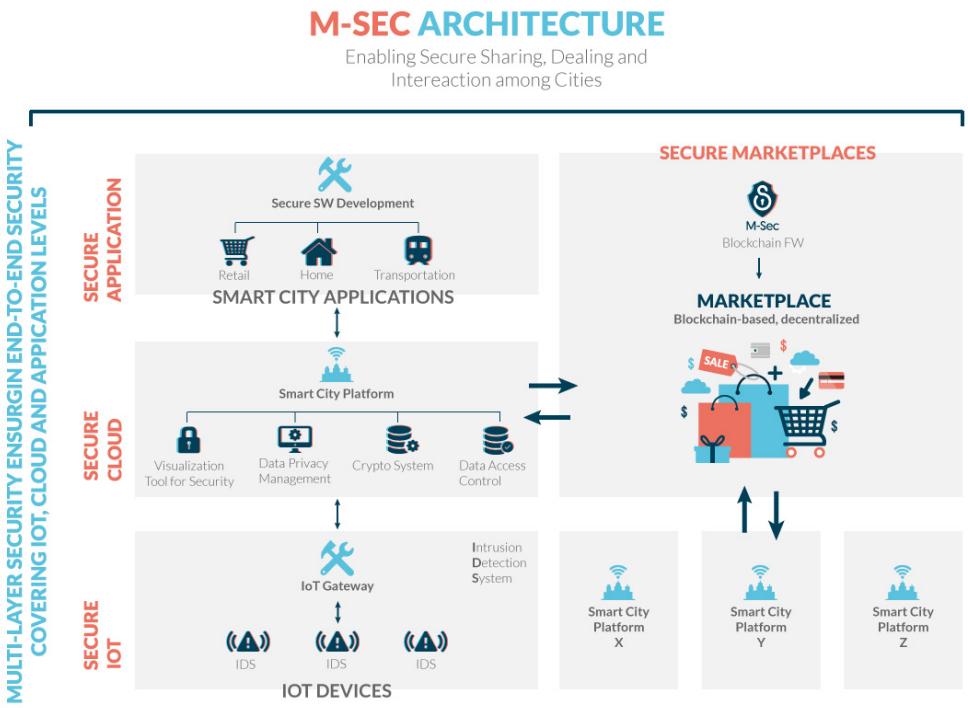

Figure 2–1. High level view of M-Sec architecture

2.2 Which will be M-Sec's main results?

M-Sec will achieve 4 main results:

M-Sec IoT Infrastructure

The M-Sec smart city platforms will be distributed and robust, and based on IoT, cloud, Big Data and blockchain technologies. Through this trusted infrastructure, IoT stakeholders will be empowered to develop and operate new IoT applications for smart cities on top of smart objects. Follow our pilots in real-life smart cities: Santander (Spain) and Fujisawa (Japan)!

M-Sec Smart City Ecosystem

Build and experiment with new ideas and application services for smart cities! Startups, SMEs and developers will be connected to the M-Sec actors and be given access to a complete set of tools and infrastructures.

M-Sec Marketplace

Our open market of applications, data and services will facilitate the exchange of value and information between IoT devices and people through virtual currencies. Check the incentives that motivate the interaction between smart objects and humans.

M-Sec Replication Plan

Learn how to replicate the M-Sec approach in your city! Our revenue model will guarantee the return on investment and all M-Sec benefits.

3. Significant problems that Internet of Things face

In addition to conventional internet connected terminals, such as personal computers and smartphones, various things around the world, such as home appliances, automobiles, buildings and factories, are connected to the internet, and the number has exploded. According to a new forecast from International Data Corporation (IDC), the number of devices connected to the Internet, including the machines, sensors, and cameras that make up the Internet of Things (IoT), continues to grow at a steady pace. It is **estimated that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data in 2025[1].**

By installing sensors and processors that process communication functions and information, new value will be added. A variety of applications are being considered, such as health management using wearable devices, and maintenance and management using sensors in places where it is difficult for human eyes to work or work. First of all, the number of “consumers” and “communication” that proceeds is large at more than 5 billion, and the annual growth rate is expected to be around 10%. In particular, "consumers" are approaching the scale of the world's population of approximately 7 billion.

Combatting cybersecurity risks has grown in importance with the evolution of the digital economy. The World Economic Forum published The Global Risks Report 2019 in January 2019[2]. The report identifies, as global risks, large-scale phenomena with the potential to cause large-scale damage worldwide in the next 10 years. The report organizes these risks by their potential likelihood, their impact, and their interconnections.

According to the report, among the global risks that affect multiple domains, (such as economics, society, environment, and technology) cyber-attacks, critical information infrastructure breakdowns, data fraud or theft, and security threats are ranked among the highest in likelihood and impact.

Examining the interconnections among risks shows that cyber-attacks are related not only to data fraud and critical information infrastructure breakdowns, but also to profound social instability, interstate conflict, and failure of national governance

Cybersecurity vulnerabilities and impacts are anticipated to spill out of cyber spaces and affect the real world, as the IoT becomes more prevalent. The IoT and related matters have been moving up in the ranks of cybersecurity trends mentioned above. **The NICTER Analysis Report 2018**, released by the National Institute of Information and Communications Technology (NICT) in February 2019, **listed the top 10 Technology Advancement destination port numbers targeted in major cyber-attacks measures** by NICTER. **Eight of the 10 ports were associated with IoT devices such as web cameras and home routers.** Even the

[1] https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[2] https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2019/chapter-1.pdf#page=9

category of Other Ports contains many ports used by IoT devices, such as ports used by online management interfaces for equipment and machines. Therefore, addressing IoT device vulnerabilities has become increasingly important, as IoT turns into a new platform for cybersecurity threats.

According to IoT Analytics Research, **IoT security spending was estimated at $703M for 2017 and the fast growing market (CAGR of 44%)** is forecasted to reach almost a $4.4B opportunity by 2022, as shown in the figure below.

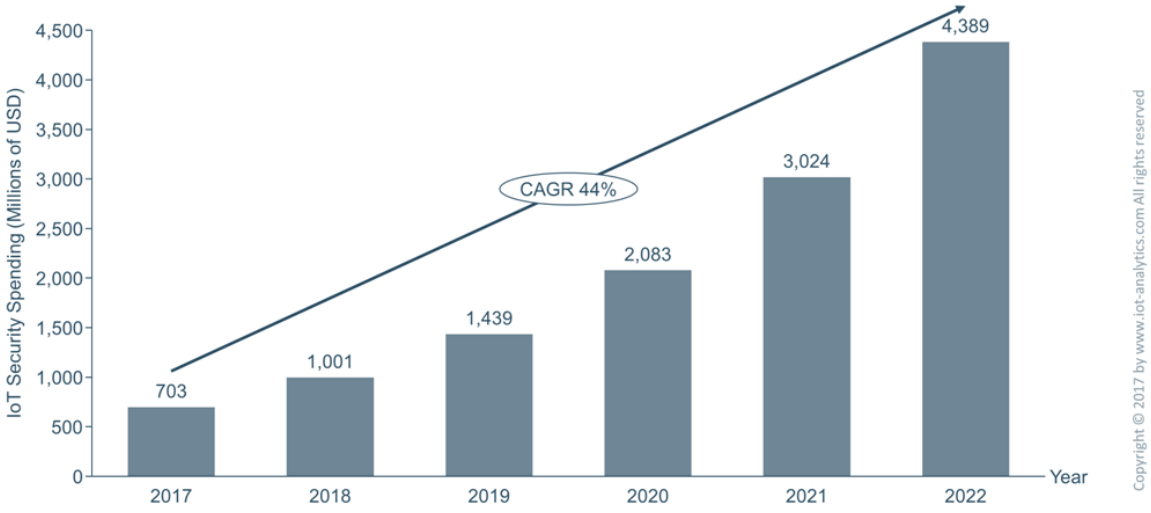

Figure 3–1: IoT Security Market-Total Market ($M)

In addition, the same source (IoT Analytics Press Research) released that the **most common IoT breaches that happened between 2015-2017 were caused by malware (24%), followed by human's factor "man in the middle" (22%), brute force (18%) and denial of service (15%).**

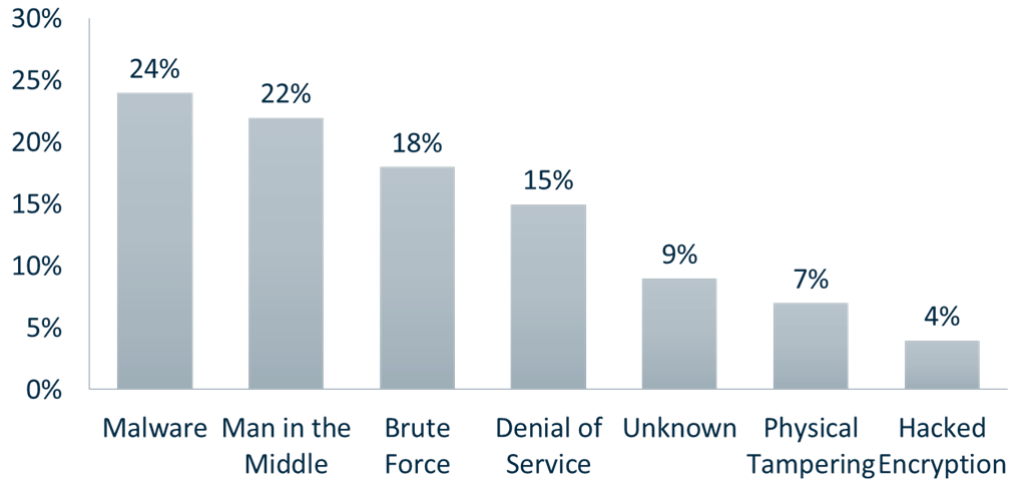

Figure 3–2: Most Common IoT breaches (2015-2017)

4. Background Analysis

Requirements analysis & Threat Analysis play an important role for the whole lifecycle of the M-Sec project. It is the input for the M-Sec specification and overall architecture as well as for the validation of the final system and its evaluation against the desired functionality or mitigated risk.

4.1 Requirement Analysis

The requirements elicitation process conducted relies heavily on the involvement of the stakeholders in the whole value chain that the project brings. It should be noted that the M-Sec consortium includes all necessary stakeholders of the M-Sec value chain. In particular, the consortium includes smart city infrastructure providers, technology providers as well as service providers and integrators and end users. This approach allows for a credible validation of the M-Sec concept, along with different deployment configurations and services operations plans.

The analysis focused on requirements from potential end-users of the M-Sec platform, including both corporate users and citizens. A variety of modalities was exploited towards eliciting requirements, including review of the state-of-the-art services and direct contact with all stakeholders that comprise the M-Sec value chain. Direct contact with stakeholders was pursued based on the partners' business networks, involving experts from the large industrial partners of the consortium.

In parallel, the consortium partners gave an overview of the technologies involved in the project and the perspective of using them in order to implement the M-Sec concept.

The following tables present the distribution of requirements extracted among all the Categories, Types, and Groups.

Table 1: Requirement's elicitation by category

Category	Requirements	Total	%
Functional	R1.*-*.*-*	57	41
Non-Functional	R2.*-*.*-*	82	59
		139	100

Table 2: Requirement's elicitation by type

Category	Requirements	Total	%
Core System	R*.1.*-*.*-*	62	45
Pilot System	R*.2.*-*.*-*	45	32
Assets	R*.3.*-*.*-*	32	23
		139	100

Table 3: Requirement's elicitation by Group

Category	Requirements	Total	%
Data Types & Devices	R*.*.1-*.*-*	15	11
Applications, UIs, Events & Notifications	R*.*.2-*.*-*	11	8
Data Storage, Transfer & Access	R*.*.3-*.*-*	16	12
Processing, Analytics & Visualisation	R*.*.4-*.*-*	8	6
Development, Reusability & Exploitability	R*.*.5-*.*-*	27	19
Security/Privacy	R*.*.6-*.*-*	62	45
		139	100

Regarding the requirements analysis per se, quite many interesting results were extracted. For example, it has been identified that 30% of the requirements are "fundamental" ones (coming from end users, city authorities, legislation, project's objectives), with the rest of them being technical ones (coming from the partners and solution providers). Also, it was noted that about half of the requirements were extracted "internally" (from the consortium partners as a source), while the rest are based on external input.

4.2 Threat Analysis

An IoT system such as the one discussed by M-Sec includes different pieces of devices and software, ranging from IoT devices (e.g. sensors) and cloud servers, to user-side mobile devices. There is a need to conduct a multi-dimensional threat and risk assessment that can provide solid ground for multi-layered security in M-Sec. For that, the threat model selected has been STRIDE . STRIDE is a model of threats developed by Praerit

Garg and Loren Kohnfelder at Microsoft[3] for identifying system or computer security threats. It provides a mnemonic for security threats in six categories.

The threats are:

- Spoofing
- Tampering
- Repudiation
- Information disclosure (privacy breach or data leak)
- Denial of service
- Elevation of privilege

M-Sec partners decided to use STRIDE for evaluating threats against each entry point. This has helped to identify, assess, and classify potential weak areas or threat vectors and risks more granularly with respect to M-Sec IoT, cloud, and application layers

Risks are categorized into IoT (edge), communication, cloud, and application parts and they all will follow the STRIDE guidelines. Identifying the security risk area each of them affects to and specifying the information security attribute that particular threat points to, according to the qualities desirables for Information Systems of Confidentiality, Integrity and Availability (CIA).

All in all, up to 97 threats are considered and rated, therefore assigning them a certain priority in what regards the required action to solve them. A summary of some of them, can be checked in Figure 4–1 in the next page.

[3] https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/

THREAT #	DESCRIPTION	STRIDE THREAT CLASS	TYPE	SUB-TYPE	INTERFACES	M-SEC ASSET	SOURCE	PROBABILITY	CRITICALITY	RATING
Thr.IoT.1	Data stored in the device can be read by an intruder	I	IoT/Edge	Device	P1, DF1, DS1	EnMon, Crow, Caburn	Use Case 1, 2	3	3	9
Thr.IoT.2	An unauthorized party can modify data on the device	T	IoT/Edge	Device	P1, DF1, DS1	EnMon, Crow, Caburn	Use Case 1, 2	3	3	9
Thr.IoT.17	Nobody is responsible for system management and maintenance (e.g. system: device network)	Management issue	IoT/Edge	Management	Life Cycle	EnMon, Crow, KEIO Mobile Sensing Platform,Caburn IoT Devices	Use Case 1, 2, 3	1	3	3
Thr.IoT.18	Attack on Power Management …	D	IoT/Edge	Device	Device HW	Crow, KEIO Mobile Sensing Platform, Caburn IoT Devices	Use Case 1,2,3	3	3	9
Thr.Com.2	Unrestricted access to alter device configuration	T	Communication	Device	DF3	IoT Gateway, Caburn	Use Case 2, 3	3	5	15
Thr.Com.3	Data storage is readable without authentication	I, E	Communication	Data	DF4	IoT Gateway, EnMon, Crow, Caburn	Use Case 1, 2, 3	3	3	9
Thr.Com.4	Data storage is writeable without authentication	T, E	Communication	Data	DF4	IoT Gateway, Caburn	Use Case 2, 3	3	3	9
Thr.Com.5	IoT physical interfaces (USB dongles, etc.) are removed	D	Communication	Device	P2	IoT Gateway	Use Case 3	5	5	25
Thr.Com.6	Device is removed or put out of range	D	Communication	Device	DF3, P2	IoT Gateway, EnMon, Crow, Cabrun	Use Case 1, 2, 3	3	5	15
Thr.Com.7	Gateway is unplugged to free a power plug	D	Communication	Device	P2	IoT Gateway, Caburn	Use Case 2, 3	5	5	25
Thr.CD.5	Data (raw & processed, personal data) stored in the cloud can be read by an intruder	I	Cloud	Data Access, Storage	DS3	SoxFire, Companion DB	Use Case 2, 3	3	5	15
Thr.CD.6	An unauthorized party gets access to device configuration information	I	Cloud	Data Access	DS3	SoxFire	Use Case 3	1	3	3
Thr.App.1	Libraries and modules on which the application is reliant, can be compromised or replaced by malicious versions. (they can be affected by the same threats as the application itself)	S, D, T	Application	App	Lower Levels, DS4, communication links, Digital assets, Application Logic		All Use Cases	1	3	3
Thr.App.2	Other malicious agents can issue requests and data on behalf of the application.	S (e.g. IP Spoofing)	Application	App	DF7, DF9, DS4, Digital Assets, Application Logic	Connected Care	Use Case 2	3	5	15

Figure 4–1: Summary of some of the threats identified

Once the threat analysis process was completed, there was the chance to discuss the components, techniques and methods that will help M-Sec to proceed with the risk mitigation and achieve a substantial drop in the corresponding risk rating.

In an effort to keep the consistency, these mitigation activities link to every threat in the lists previously presented. Therefore, it requires covering the mitigation activities that will be put in place in such diverse areas as the IoT layer, the communication, and cloud and application levels, comprising the whole end-to-end risks mitigation.

When dealing with risks mitigation related to privacy, GDPR (General Data Protection Regulation), APPI (Act on the Protection of Personal Information) and ethics, it is worth noting that everything done should go attached to the principles of privacy by design, and each M-Sec use case must in the end comply with the Privacy Compliance that will be evaluated by the corresponding Data Protection Officer (DPO). Nevertheless, readers are invited to check Deliverable 5.11 “M-Sec GDPR compliance assessment report” out and find there the activities applied in the diverse use cases to fulfil this alleviation of threat level in relation to privacy.

All in all, the consortium conducted thorough analysis and evaluation of all the threats looming over M-Sec and came up with a series of mitigation activities such as the ones that appear collected in the selection presented in Figure 4–2.

THREAT #	DESCRIPTION	STRIDE THREAT CLASS	TYPE	SUB-TYPE	INTERFACES	M-SEC ASSET	SOURCE	PROBABILITY	CRITICALITY	RATING	COMMENTS / MITIGATION
Thr.IoT.1	Data stored in the device can be read by an intruder	I	IoT/Edge	Device	P1, DF1, DS1	EnMon, Crow, Caburn	Use Case 1, 2	3	3	9	TPM will be designed to reduce the probability by securing the IoT device itself.
Thr.IoT.2	An unauthorized party can modify data on the device	T	IoT/Edge	Device	P1, DF1, DS1	EnMon, Crow, Caburn	Use Case 1, 2	3	3	9	TPM will encrypt data to reduce this risk.
Thr.IoT.17	Nobody is responsible for system management and maintenance (e.g. system: device network)	Management issue	IoT/Edge	Management	Life Cycle	EnMon, Crow, KEIO Mobile Sensing Platform,Caburn IoT Devices	Use Case 1, 2, 3	1	3	3	M-Sec partners will play this role and assign a responsible person. Partners has already assigned their responsibles for the maintenance to lower the likelihood and impact.
Thr.IoT.18	Attack on Power Management …	D	IoT/Edge	Device	Device HW	Crow, KEIO Mobile Sensing Platform, Caburn IoT Devices	Use Case 1,2,3	3	3	9	No Firmware or data storage. Physical security & clamping to mitigate risk by lowering likelihood.
Thr.Com.2	Unrestricted access to alter device configuration	T	Communication	Device	DF3	IoT Gateway, Caburn	Use Case 2, 3	3	5	15	Authentication & physical security
Thr.Com.3	Data storage is readable without authentication	I, E	Communication	Data	DF4	IoT Gateway, EnMon, Crow, Caburn	Use Case 1, 2, 3	3	3	9	Authentication & Encryption
Thr.Com.4	Data storage is writeable without authentication	T, E	Communication	Data	DF4	IoT Gateway, Caburn	Use Case 2, 3	3	3	9	Authentication & Encryption
Thr.Com.5	IoT physical interfaces (USB dongles, etc.) are removed	D	Communication	Device	P2	IoT Gateway	Use Case 3	5	5	25	Physical security & interfaces to be clamped and locked
Thr.Com.6	Device is removed or put out of range	D	Communication	Device	DF3, P2	IoT Gateway, EnMon, Crow, Cabrun	Use Case 1, 2, 3	3	5	15	Physical security & device to be clamped and locked. Few affected devices not critical.
Thr.Com.7	Gateway is unplugged to free a power plug	D	Communication	Device	P2	IoT Gateway, Caburn	Use Case 2, 3	5	5	25	Cables to be clamped and locked
Thr.CD.5	Data (raw & processed, personal data) stored in the cloud can be read by an intruder	I	Cloud	Data Access, Storage	DS3	SoxFire, Companion DB	Use Case 2, 3	3	5	15	Encryption
Thr.CD.6	An unauthorized party gets access to device configuration information	I	Cloud	Data Access	DS3	SoxFire	Use Case 3	1	3	3	Protected in Keio's network
Thr.App.1	Libraries and modules on which the application is reliant, can be compromised or replaced by malicious versions. (they can be affected by the same threats as the application itself)	S, D, T	Application	App	Lower Levels, DS4, communication links, Digital assets, Application Logic		All Use Cases	1	3	3	Vulnerability Assessment
Thr.App.2	Other malicious agents can issue requests and data on behalf of the application.	S (e.g. IP Spoofing)	Application	App	DF7, DF9, DS4, Digital Assets, Application Logic	Connected Care	Use Case 2	3	5	15	Companion DB may mitigate some of the risks; the application will not know the keys, only the user will know it. Authentication mechanism.

Figure 4–2: Summary of some of the mitigation actions to cover threats identified

5. M-Sec Solution: A multi-layer secure IoT framework compatible with the transfer and processing of personal data between EU & JP

The main goal of M-Sec project is to research, develop, deploy and demonstrate multi-layered Security technologies to ensure hyper connected smart cities and empower IoT stakeholders with an innovative platform which leverages blockchain, Big Data, Cloud and IoT security, upon which they can build innovative smart city applications.

The project explores secure, interoperable interactions between IoT elements based on a holistic secured cloud/edge/IoT context within a future smart city. Overall, the M-Sec paradigm complements mainstream IoT/cloud technologies, through enabling the introduction and implementation of specific classes of applications and services, which are not efficiently supported by state-of-the-art architectures.

5.1 What M-Sec offers in terms of security?

The Internet of Things (IoT) has changed the way people interact with technology, and IoT security is a growing concern that is reaching a boiling point as of today.

People's connected devices are data collectors. The personal information collected and stored with these devices — such as user name, age, e-mail addresses, health data, location, and more — can aid criminals in stealing their identities.

At the same time, IoT is a growing trend, with a stream of new products hitting the market. But here's the problem: When you're connected to everything, there are more ways to access your information. That can make you an attractive target for people who want to make a profit off of your personal data.

In modern smart city applications, there is an emerging need of end-to-end security since many data sources may contain sensitive information that raises issues on privacy and data protection. The smart city application is inherently multi-layered including edge, cloud and application layers. The security and privacy issues should be addressed in the all layers to ensure "end-to-end security and privacy". However, one of the main challenges is to provide end-to-end security in the whole IoT ecosystem, since there are too many parties involved on the IoT application provided (from IoT vendors to cloud and application providers). Lately, there have been new solutions coming to the market that offer an end-to-end approach by establishing major partnerships with different players specialized on different IoT layers.

Within this context, M-Sec's aim is to provide a low-cost and flexible end-to-end secure IoT Framework extending security mechanisms from the device to the cloud and to the application, in a seamless and fully integrated manner.

M-Sec provides different components developed on each of the IoT Ecosystem layers; IoT Layer, Cloud Layer, Middleware Layer, Application Layer and Cross Layer, addressing the above-mentioned challenges by enabling security-by-design via proven technologies to secure the exchange between data from IoT devices to remote distributed entity in the cloud.

The data security methods rely on both software and hardware technologies for providing confidentiality, integrity, availability, and privacy.

As hardware based solution, the M-Sec solution provides a **Secure Element for devices based on a technique to increase the security level of a physical object via an extension conforming to the "TPM"** (Trusted Platform Module) profile standardized by the TCG (Trusted Computing Group), similar to a trust anchor. The security in question primarily relates to the integrity of the product to ensure that the product has not been compromised to extract sensitive information such as private keys or other authentication information with nuisance capability. These integrity checks can be done at different levels depending on the type of targeted platform: boot loader, Operating System (OS), and applications.

Strong authentication and encryption is designed to take into account data traversing through the cloud and getting exposed to cyber-attacks. In order to stay vigilant, cyber threats are monitored and the availability of data is ensured by enabling quicker responses. M-Sec has adopted a **lightweight Intrusion Detection System (IDS) for providing security to the IoT devices layer along with OS hardening**. OS hardening helps in reducing attack surface by closing all the ports that are not needed. This way, it is possible to monitor threats as well as prevent known attacks without consuming too much resources of the IoT devices.

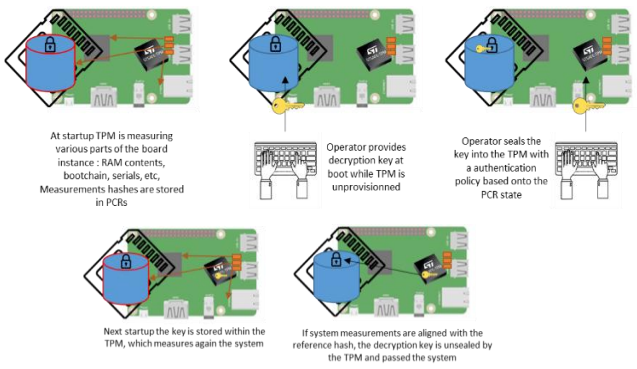

Figure 5–1: Secure Element Prototype

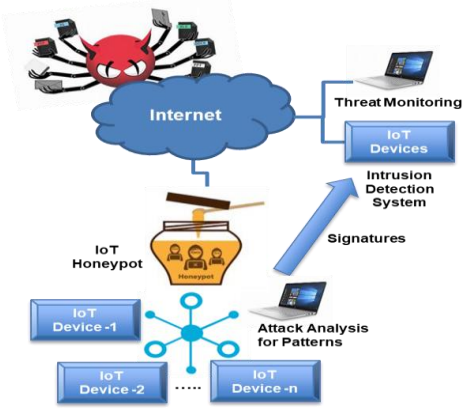

Figure 5–2: IDS Prototype

Furthermore, a **privacy management tool (Ganonymizer) has been developed to help in enforcing GDPR/PIPA compliance on video images by removing sensitive data.** Hence, the M-Sec developed solution enhances the security of data between the devices and their respective back-ends in complementary ways.

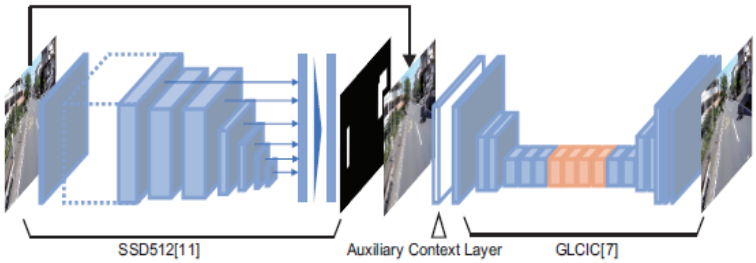

Figure 5–3: Ganonymizer Prototype

In the Middleware Layer, the current situation presents an increasing number of smart city platforms being proposed by different vendors. However those **solutions are often locked-in by design and can't share data with one another, which causes market fragmentation and poor user experience**. M-Sec proposes two tools for city data access. On the one hand, **sensiNact which** is designed to allow those platforms to **interoperate**, thus **coexist** and **benefit** from the richness of the variety. SensiNact **provides a fine grained security mechanism to allow access to services by only authentified and authorised entites**. The second one is **KEIO SOXFire** which provides **practical distributed and federated infrastructure for IoT sensor data sharing among various users/organizations** in a way that is scalable, extensible, easy to use and secure while preserving privacy.

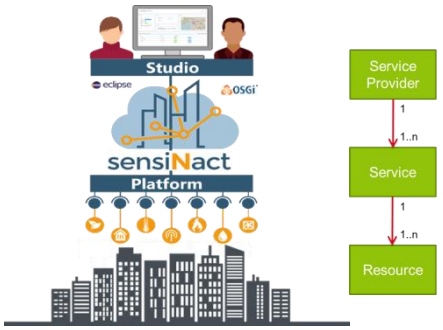

Figure 5–4: Sensinact Prototype

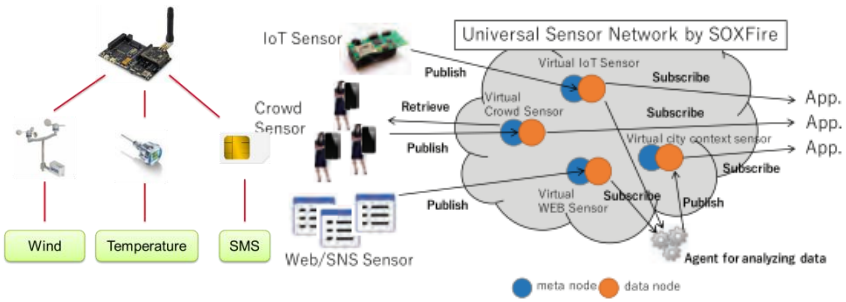

Figure 5–5: Keio SOXFire Prototype

M-Sec also entails data security where sensitive data is encrypted together with a hash. Thanks to the M-Sec Blockchain and Middleware, the synergy between on-chain and off-chain data and access control becomes possible. The crypto companion DataBase is a system that encrypts the data with an asymmetric public/private key pair. The data can only be accessed by the owner who has to be authenticated, and the authorised operators allowed by the owner. **Sensitive data is encrypted together with a hash for data tamper proof purposes.**

At an application level, M-Sec provides methodologies and tools to develop smart city applications in order to support developers of smart city applications. The project proposes a framework for building a body of

knowledge and a knowledge base for secure software development. This **framework provides security requirements modelling support system (Security analysis tool) and a Modal System Transition Analyser to eliminate both human errors in designing the application logic and a wide number of tests performed to verify the security level.**

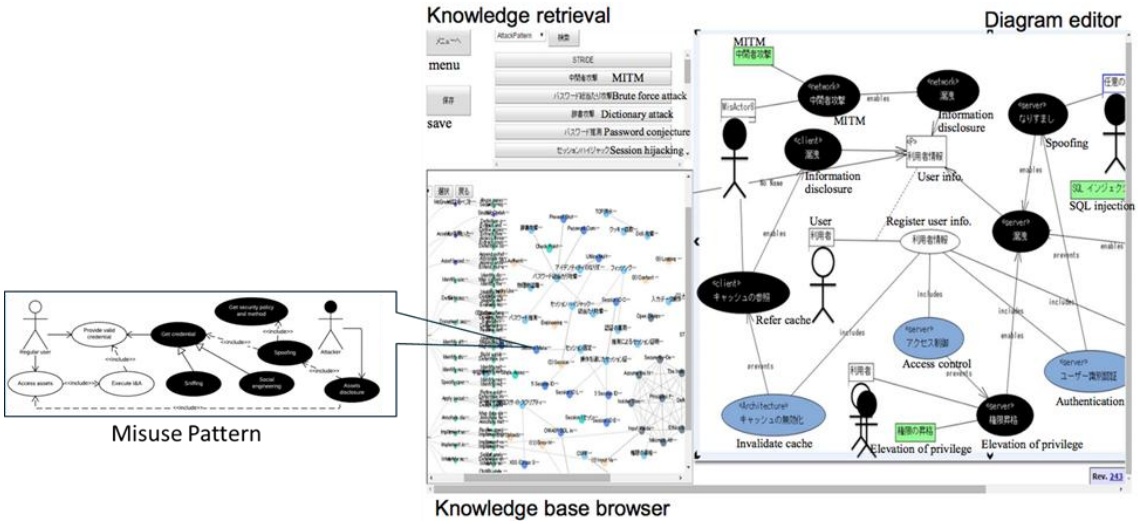

Figure 5–6: Security Analysis Tool Prototype

Finally, at the cross layer, a Security Management Tool ensures a secured and smooth interoperation for each of the elements of the architecture. The Security Management Tool provides a directory service containing all information to manage security services for clients, such services known as AAA for Authentication, Accounting and Authorization. The security Manager is a set of centralised security functions that are necessary to ensure end-to-end security, privacy and therefore digital trust. It is designed to support several security functionalities aggregated in a single backend using the Lightweight Directory Access Protocol (LDAP) standard.

In the Figure 5–7 below, the end-to-end security value added by M-Sec through the different layers is shown.

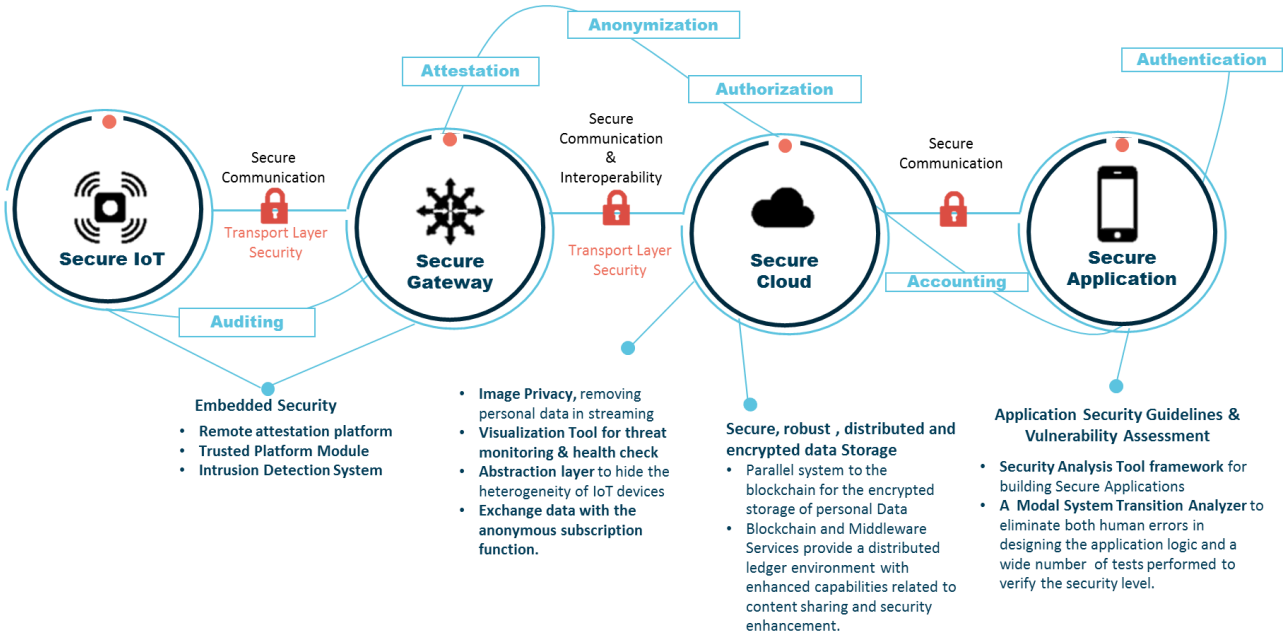

Figure 5–7: M-Sec end-to-end approach

5.2 Enabling the creation of liquid markets

One of the main goals of M-Sec is to create decentralised IoT ecosystems and validate their viability and sustainability. To this direction, we defined and implemented a novel marketplace where smart objects can exchange information and services through the use of virtual currencies allowing real-time matching of supply and demand, enabling the creation of liquid markets with profitable business models of the IoT stakeholders. Market participants, from IoT devices to humans using mobile applications are able to exchange data and value through the M-Sec blockchain implementation. The owner of a sensor/data source who wishes to make their data available for purchase or exchange can register to the dedicated created smart contract providing information about the type of the data, their frequency, the price, the location etc. Then, a user of the M-Sec Platform who acts here as a potential buyer using our developed front-end can see all the available sensors and their data. Upon finding some interesting data they can retrieve additional detailed descriptions about them and then buy the data of interest using M-Sec Tokens, which is a crypto currency in the form of a smart contract running in on blockchain presented in previous section. The deployed smart contracts communicate with each other to verify the sufficient funds of the buyer and complete the purchase by transferring funds from the balance of the buyer to the one of the data owner.

Furthermore, thanks to the Trust and Reputation (T&R) model developed within the M-Sec scope, it is possible to; 1. Collect information about a certain participant in the community by asking other users their opinions or recommendations about that peer; 2. Aggregate all the received information properly and somehow computing a score for every peer in the network; 3. Select the most trustworthy or reputable entity in the community providing a certain service and effectively having an interaction with it, assessing *a posteriori* the satisfaction of the user with the received service; 4. Punish or reward according to the satisfaction obtained, adjusting consequently the global trust (or reputation) deposited in the selected

service provider. The T&R engine is used on top of the Blockchain Middleware Services and the IoT Marketplace. Such an engine would enhance the security mechanisms of M-Sec and make it possible to evaluate the actual content being shared through the Blockchain and the Marketplace, thus ensuring the trustworthiness of the several actors participating in the exchange or sharing of information, data and services.

5.3 M-Sec Architecture overview

The methodology employed is based on the 5W1H approach. The 5W1H (Five Ws and How, 5W1H, or Six Ws) are questions whose answers are considered basic in information gathering or problem solving. They are often mentioned in journalism, research and police investigations. According to the principle of 5W1H, a report can only be considered complete if it answers these questions starting with an interrogative word: Who, What, When, Where, Why, and How.

The “problem” to be solved in the case of this task is the definition of the M-Sec System Architecture. The five Ws and 1 H are asked for each and every identified component (asset), and thus the corresponding steps also take place, having on their centre each component (and in some cases, specific groups of components and sub-systems). The aggregation of the answers to those questions provided the final results for the definition of the M-Sec system as a whole. **The final result is a mixed view, since it combines the layered view (Where) with the FGs one (What).**

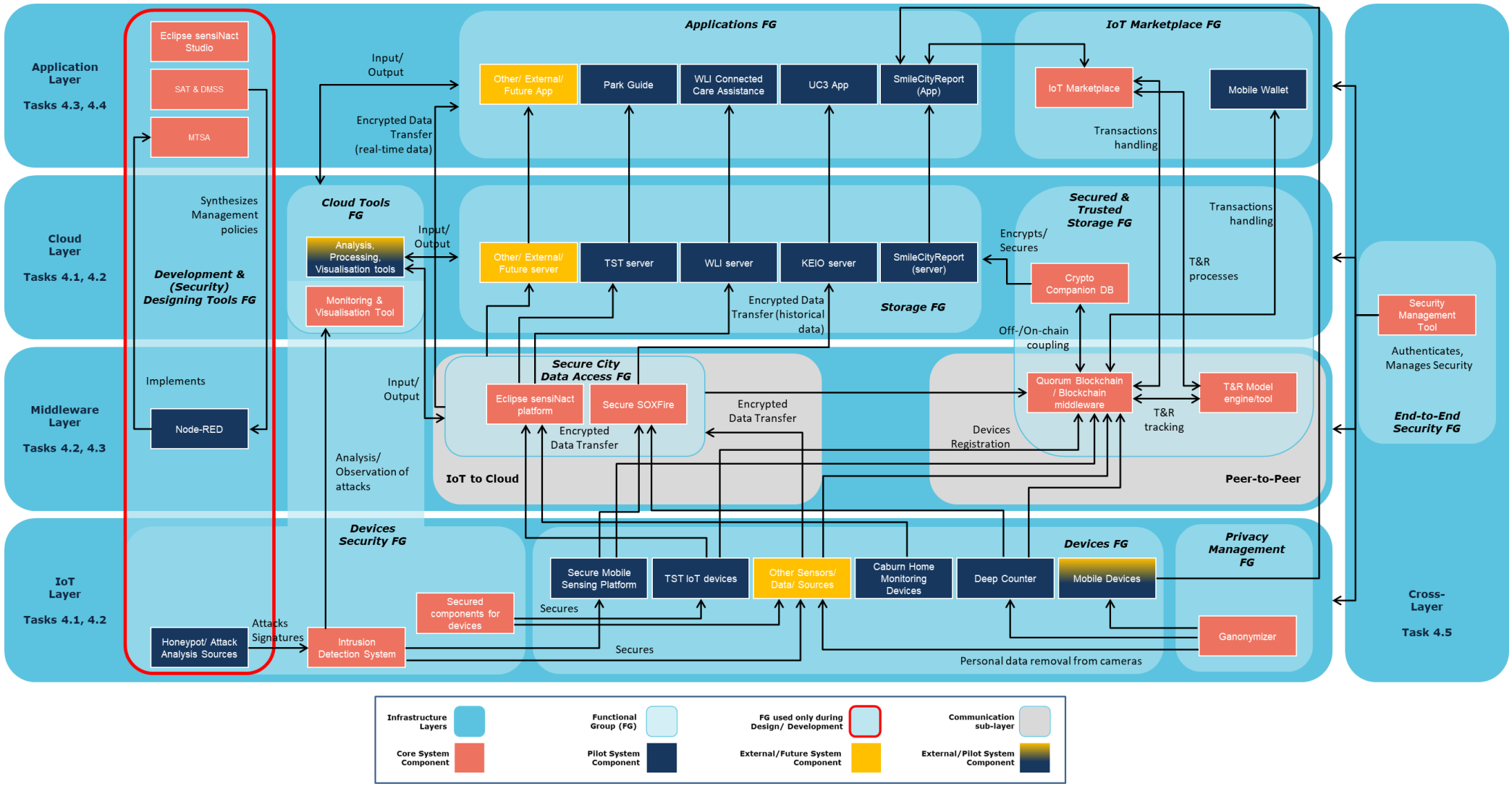

Figure 5–8: M-Sec System 5W1H analytical global Architecture View

6. Conclusion

This White paper reports the work done in the H2020 M-Sec project towards fostering the collaboration between the JP and the EC in the advance of Multi-layered Security technologies to ensure hyper-connected smart cities with Blockchain, Big Data, Cloud and IoT.

This White paper presents the challenges in terms of security faced by the IoT market and the solution offered by the M-Sec Project. The methodology that has been followed for the analysis and design of M-Sec is extensively described. The M-Sec architecture has covered all aspects of the 5W1H principle. M-Sec components are described and grouped in relevant functional groups, taking under consideration the User Requirements and Use Cases and were separated in layers. Also, the links between all components were identified.

Furthermore, in this report the consortium presents a summary of the threats analysis methodology applied, introducing which kind of model is applied and how, along with detailed lists of potential threats that may affect the different layers in the M-Sec architecture.

Several threats looming over the M-Sec framework have been distinguished when carrying out this exercise, affecting the layers the M-Sec framework is composed of and making it clear some of those threats could turn into a real relevant risk and may require a prompt action to alleviate them. Therefore, during the execution of the different M-Sec use cases, diverse mitigation activities will be put into effect aiming at lowering those threats probability and criticality, and thus making the risk negligible.

Some of these mitigation activities are somehow linked to the so-called privacy enhancing technologies, which have also received their share of attention and will play an important role in executing the project's use cases in a format that ensures the security and privacy of data and users.