SUSTAIN Deliverable

D7.1 Functional requirements from the market analysis for the different technologies developed in WP2-WP6

Grant Agreement number	101071179
Action Acronym	SUSTAIN
Action Title	Smart Building Sensitive to Daily Sentiment
Type of action:	HORIZON EIC Grants
Version date of the Annex I against which the assessment will be made	28th March 2022
Start date of the project	1st October 2022
Due date of the deliverable	M12
Actual date of submission	18th January 2024
Lead beneficiary for the deliverable	AALTO
Dissemination level of the deliverable	Public

Action coordinator's scientific representative

Prof. Stephan Sigg
AALTO –KORKEAKOULUSÄÄTIÖ,
Aalto University School of Electrical Engineering, Department of Communications and Networking
stephan.sigg@aalto.fi

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Innovation Council and SMEs Executive Agency (EISMEA). Neither the European Union nor the granting authority can be held responsible for them.

European Innovation Council

Authors in alphabetical order		
Name	**Beneficiary**	**e-mail**
Name (from A's to Z's)	SHORT name of organization	name.name@org.de
Andraud, Martin	AALTO	martin.andraud@aalto.fi
Gasulla, Manel	UPC	manel.gasulla@upc.edu
Iacca, Giovanni	UNITN	giovanni.iacca@unitn.it
Kahraman, Nihan	YTU	nicoskun@yildiz.edu.tr
Ma, Xujun	IMT	xujun.ma@telecom-sudparis.eu
Sigg, Stephan	AALTO	stephan.sigg@aalto.fi
Zhang, Daqing	IMT	daqing.zhang@telecom-sudparis.eu

Abstract
The work of WP7T1 is reported in two Deliverables, D7.1 and D7.2, the latter being due M36. D7.1 is due M12 and marks the first steps of this work. Deliverable D7.2 will contain the results from the appropriation study and market analyses per technology. The AALTO PI research team is collaborating with the Aalto School of Business Department of Information System Science in this work with regard to WP7T1. WP7T1 conducts market analyses for the different technologies developed in WP2-WP6. The technologies are as follows: 1) intelligent reconfigurable circuits (WP2), 2) privacy scalable massive communication (WP3), 3) Awareness supporting global sentiment sensing (WP4), 4) as well as energy harvesting (WP5) and 5) behavior-based security (WP6). The aim of D7.1 is to establish a plan for the market analyses per technology. The analyses may include identifying reference markets, market size and market needs. The market analysis per technology needs to be adapted as the technologies form a diverse set. In addition, the competitive edge of each technology will be identified for each technology to assess its standing against other alternative solutions. Barriers to market entry will also be analysed.

Contents

1 Intelligent Reconfigurable Circuits and systems (WP2)

The area of intelligent reconfigurable circuits encompasses a large variety or markets and applications, thus we will start by clarifying the intended terms here. First, the term "circuits" focuses on electronic circuits and systems, found in what is generally referred to the Internet of Things, or IoT. IoT devices are typically small interconnected devices, used in a wide range of applications, ranging from industry, automotive, consumer wearables to biomedical monitoring. The IoT market witnesses an incredible growth, from around 300 billion dollars in 2021 to an expected 650 billions dollars in 2026, corresponding to around 16% yearly increase (https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html). This is mainly due to a continuously increasing need in automation and remote monitoring applications, offered by low-cost IoT sensing technologies. Second, the term "intelligent" refers to IoT devices that are able to perform a variety of tasks related to sensing, monitoring, alerting and controlling various systems around us. Among this booming market, the sustAIn project is generally targeting smart cities and smart building applications, where the objective is to make peoples lives safer (by monitoring their environment), greener (by minimizing resources for e.g. heating, lightning, water) or simply easier (by adapting their environment to their current emotions or needs). In particular, building automation has gained significant interest over the past years, with the concept of "Industry 4.0" [1]. It encompasses sensor monitoring for security (fire detection, gas monitoring, etc.), resource management (temperature, humidity, etc.) and other building use (parking spaces, rooms, etc.). It is a market with an expected 11% growth over the next years (https://www.mordorintelligence.com/industry-reports/smart-building-market). In Europe, the number of active connections in smart buildings through IoT devices is expected to grow from 65 million in 2022 to 154 millions in2026 (Source: European Telecommunications Operators Network). For instance, raising energy costs and sustainability issues are an increasing concern, requiring automated and smart solutions. This requires "reconfigurable" systems, able to analyse the current environment conditions and act accordingly, differently for each user or group of users. This is one main objectives of sustAIn.

[1] Anurag Verma, Surya Prakash , Vishal Srivastava, Anuj Kumar, and Subhas Chandra Mukhopadhyay, "Sensing, Controlling, and IoT Infrastructure in Smart Building: A Review" IEEE sensors, 2019

2 Awareness supporting Distributed Intelligence (WP3)

Distributed intelligence solves complex learning and decision-making problems, where processing may inherently be in parallel. To support awareness, information from sensing sources is processed through distributed intelligence.

Supporting Technology: real-time process control, leader election, consensus mechanisms, distributed search and discovery, spanning tree generation, resource allocation, distributed learning, blockchain, encryption.

Market impact:

- **Applications**: This technology is used in Edge and Federated learning schemes that inhibit distribution of clients. Through the integration of intelligence into communication networks, specifically in cellular networks (AI in networking), multiple new application areas are opened
- **Market Size**: The market for distributed intelligence is significant as the computational load may be spread across multiple constrained devices and also towards the edge or cloud.
- **Challenges**: Challenges include resource gentle cryptographic routines, consensus mechanisms, as well as the privacy and security issues due to the sharing of data.

3 Awareness Supporting Global Sentiment Sensing (WP4)

Market analysis for sentiment sensing technologies could be broken down into various technologies, e.g., text-based sentiment analysis, video-based sentiment analysis, speech-based sentiment analysis, biological signal-based sentiment analysis, and the emerging wireless-sensing based sentiment analysis. By examining those technologies and understanding their role, adoption, and potential impact in the market, we could have a much clearer outlook how will the technique developed in SUSTAIN stand in the market.

3.1 Text-based sentiment analysis

Supporting Technology: Text-based sentiment analysis leverages natural language processing (NLP) and machine learning techniques to analyze textual data and classify it into sentiment categories such as positive, negative, or neutral.

Market impact:

- **Applications**: Text-based sentiment analysis has been broadly utilized in industry applications, such as brand monitoring, customer feedback analysis, and social media sentiment tracking. It plays a vital role in finance for predicting market sentiment based on news and social media content. In customer service, it helps in sentiment-driven chatbots and email analysis.
- **Market Size**: The market for text-based sentiment analysis and services has been growing steadily. It includes both standalone sentiment analysis solutions and NLP APIs offered by major tech companies, including Google, Microsoft, IBM, etc.
- **Challenges**: Text-based sentiment analysis needs to deal with context of violence and irony, as well as privacy and ethical concerns related to data handling.

3.2 Video-Based Sentiment Analysis

Supporting technology: Video-based sentiment analysis combines computer vision and audio processing to excavate visual and auditory details from video content, including facial expressions, body language, and speech.

Market impact:

- **Applications**: Video-based sentiment analysis is gaining attraction in media and entertainment for understanding audiences' reaction to movies and TV shows. It is also used in healthcare for telemedicine to assess patients' emotion.
- **Market Size**: The market for video-based sentiment analysis is growing rapidly as video content becomes increasingly popular across numerous platforms like YouTube and TikTok. Meanwhile, media companies, advertisers, and content creators are also interested in understanding the impact of their content on audiences' emotion.
- **Challenges**: Challenges lie in ambient light condition, camera angles, and cultural context when interpreting facial expressions or body language through video. Still, the privacy issue is still an unneglectable concern.

3.3 Speech-Based Sentiment Analysis:

Supporting Technology: Speech-based sentiment analysis focuses on analyzing spoken language, including prosody (intonation, tone, rhythm), speech recognition, and audio sentiment classification.

Market impact:

- **Applications**: This technology is used in call centers for customer sentiment analysis, in voice assistants and chatbots for emotional recognition, and in healthcare for analyzing patient sentiments during voice interactions.
- **Market Size**: The market for speech-based sentiment analysis is expanding as the booming of voice-activated devices and services. Some companies also use it to enhance customer service and improve user experiences.
- **Challenges**: Challenges include accurate speech recognition, multilingual environment as well as the privacy and security issues in the use of voice data.

3.4 Biological signal-based sentiment Analysis:

Supporting technology: Biological signal-based sentiment analysis adopts contact-based medical devices (e.g., PPG, EEG, ECG, thermometer, etc.) to measure subjects' physiological signals and leverages machine-learning or deep-learning tools to further estimate people's emotion states.

Market impact:

- **Applications**: This technology has applications in healthcare, mental health, and emotion-aware human-computer interaction. It can be used to assess patient emotions, monitor stress/fatigue levels, and improve user experience in applications like virtual reality (VR) and gaming.
- **Market Size**: The market for biological signal-based sentiment analysis is growing vastly due to the increased concern addressed in mental health disclosure and prevention and the widespread digital technologies for wearable biosensors.
- **Challenges**: Challenges include accurate and user-friendly data collection, real-time signal process, and also privacy concerns when dealing with personal health data.

3.5 Emerging wireless-sensing-based sentiment analysis:

Supporting technology: Wireless-sensing-based human-activity detection relies on ubiquitous wireless devices, e.g., LoRa, RFID, Wi-Fi, 4G/5G, etc, and robust sensing algorithms. In the context of SUSTAIN project, human-centric awareness, such as human positioning and tracking, vital sign monitoring, and gesture recognition, are generated by wireless sensing techniques in smart building applications. Meanwhile, machine/deep learning algorithms are still needed to achieve real-time sentiment analysis.

Market impact:

- **Applications**: This technology can be used for eldercare, monitoring patient activities, ensuring workplace safety, enhancing the functionality of smart buildings or houses, and further estimate subjects' emotion status .
- **Market Size**: The market for wireless-sensing-based human-activity detection is growing, driven by the increasing adoption of IoT devices and smart homes. Wireless-sensing technique could greatly

protect privacy issue compared with conventional methods and achieves most comfort user experience due to its contact-free nature, and further offer opportunities for improving convenience, security, and healthcare services.

- **Challenges**: Challenges include data privacy, accuracy and signal annotating for sentiment sensing.

4 Energy Harvesting (WP5)

Buildings are evolving into smart organisms through their unmatched concentration of distributed sensing, actuation and intelligence. This requires a massive deployment of sensors of all kind. SUST(AI)N derives theoretical & experimental underpinnings to combine novel distributed intelligence, unprecedented sensing accuracy, and reconfigurable hardware in a smart building context into a conscious organism that achieves self-awareness through probabilistic reasoning across its connected sustainable devices. Sustainability is reached via **energy harvesting**, energy-less distributed processing, energy-less encrypted communication and RF-sensing. Energy harvesting will be used to power the sensors and reconfigurable hardware in the SUST(AI)N project. In a more general context, energy harvesting, which harnesses environment energy, is used to power the nodes of wireless sensor networks and more broadly and recently of the internet of things (IoT). IoT devices are used in all kind of applications and markets, e.g., industry, automotive, smart buildings, civil infrastructures and cities, traffic and goods management, consumer wearables, healthcare, environmental monitoring and precision farming, among others. In particular, building automation has gained significant interest over the past years, with the concept of "Industry 4.0" [1]. It encompasses sensor monitoring for security (fire detection, gas monitoring, etc.), resource management (temperature, humidity, etc.) and other building use (parking spaces, rooms, etc.). It is a market with an expected 11 % growth over the next years (https://www.mordorintelligence.com/industry-reports/smart-building-market). In Europe, the number of active connections in smart buildings through IoT devices is expected to grow from 65 million in 2022 to 154 millions in 2026 (Source: European Telecommunications Operators Network). For instance, raising energy costs and sustainability issues are an increasing concern, requiring automated and smart solutions. Billions of wireless sensors are expected to be installed over the coming decade, and half of those will be located inside smart buildings [2].

Energy harvesting competes with primary batteries, which provide a low-cost and long-term proven solution but have limited energy and require a periodic replacement. This replacement adds maintenance costs and, in some applications, can be even impractical or unfeasible, e.g. in remote places or embedded structures. Apart, in tiny sensor nodes, primary batteries can also constitute the largest and most expensive subsystem. Furthermore, even there are European directives about waste batteries (2006/66 and 2018/849), a sustainable and circular economy should avoid their use as much as possible. Main energy harvesting sources are radiant, mechanical and thermal. in the SUST(AI)N project light, thermal and radiofrequency (RF) harvesting technologies are tackled. Energy harvesters are composed of the energy transducer, e.g. a photovoltaic (PV) cell for light harvesters, and an ensuing power processing circuit that includes a maximum power point tracker (MPPT) to extract maximum power from the transducer. Apart from the competing primary batteries, a common major technical challenge for all energy harvesting technologies is the design of power efficient MPPTs considering the low power output of the energy transducer (e.g., <1 mW).

4.1 Indoor light-energy harvesting

Solar energy is a well stablished renewable energy. Indoors, e.g. inside buildings, light mainly comes from artificial lights and indirect sunlight. Light power density is therefore much lower with a 100 to 1000-fold reduction with respect to outdoors with direct sunlight, which poses challenges in effectively harvesting energy for powering sensor nodes.

Market Size

Considering the growth of the market for IoT hardware, the market of photovoltaic cells for indoor applications is expected to reach 1 USD billion in 2024 [2] when in 2017 just reached 140 USD million.

Technical Challenges

A particular challenge is identified: the optimal combination of cell PV technologies (crystalline and amorphous silicon-based, organic, III-V materials, DSSC and Perovskite) with the type of indoor lights, either artificial (LED, CFL, halogen) or indirect sunlight, so as to increase the power at the output.

4.2 Thermal Energy harvesting

Thermal energy harvesting will be based on thermoelectric generators (TEGs) as the energy transducers. These devices, based on the Seebeck effect, generate electrical energy from a thermal gradient between two plates where the thermoelements (N and P type semiconductors) are disposed electrically in series and thermally in parallel. So, to extract energy, a heat or cold thermal source is needed. TEGs are used in applications such medical and wearable devices, smart buildings, aeronautics and aerospace, and automobile engines, among others [3]. In buildings, heating sources like heat pipes, water heaters, central heating, and air conditioners are widely existing.

Market Size

The thermoelectric generators market is projected to grow from USD 761 million in 2022 to USD 1.23 billion by 2027 at an annual growth rate of 10.1 % (Source: MarketsandMarkets). However, powering wireless sensors in smart buildings is not mentioned as one of the applications.

Technical Challenges

A particular technical challenge is to achieve a significant thermal difference across the TEG device. Even the temperature difference between the hot/cold source and the ambient can be of several tens of Celsius degrees, it is challenging that a significant part of this temperature difference can drop across the TEG, whose thickness in commercial devices is just of a few millimetres.

4.3 RF Energy harvesting

RF energy harvesting is based on capturing energy either from RF dedicated sources, such as for RFID devices, or from the RF energy already present in the environment and coming from unintentional sources such as TV, Radio, cellular, Satellite, or WiFi emitters. In particular, RFID technology is used for tracking and identification in various industries, such as inventory management, supply chain optimization and asset tracking.

Market Size

The market for RF energy harvesting has been steadily growing across various applications, driven by the need for sustainable, low-power solutions. In IoT devices, it is expected to witness significant expansion as industries increasingly adopt IoT technologies for remote monitoring, asset tracking, and smart infrastructure. Moreover, RF energy harvesting is gaining traction in wearable electronics, environmental monitoring, and industrial automation, where the demand for energy-efficient, maintenance-free solutions is on the rise. With a growing emphasis on reducing the environmental footprint and the ongoing development of RF harvesting technologies, the market size for RF energy harvesting is anticipated to continue its upward trajectory in the coming years. Particularly, RFID technology is a well stablished technology expected to reach USD 35.6 billion by 2030 from USD 18.45 billion by 2023, thus with an annual growth rate of 11.9 % (https://www.marketsandmarkets.com/Market-Reports/rfid-market-446.html). One of the major driving factor of the RFID market is the increasing demand for inventory management and supply chain optimization in various industries such as retail, healthcare and automotive.

Technical Challenges

Harvesting RF energy from unintentional sources remain a particular technical challenge since the received power density is extremely low. Furthermore, the lower the received power the lower the efficiency of the rectenna (RF harvesting device). On the contrary, RFID tags rely on a RF dedicated source (the reader) so that enough energy is received to power them. Even so, improving the efficiency of the tag rectenna can lead to higher reading distances.

[1] A. Verma et al., Sensing, Controlling, and IoT Infrastructure in Smart Building: A Review. *IEEE sensors*, 2019.

[2] I. Mathews et al., Technology and Market Perspective for Indoor Photovoltaic Cells. *Joule*, 2019.

[3] N. Jaziri et. Al., A comprehensive review of Thermoelectric Generators: Technologies and common applications. *Energy Reports*, 2020.

5 Behavior-based Security (WP6)

5.1 Behavior Based Security Market Analysis and Size

Behavior-based security (BBS) is an approach that focuses on monitoring and analyzing user and system behavior to detect potential security threats or breaches. When conducting a market analysis for behavior-based security solutions, several critical issues and factors need to be assessed to understand the market landscape and make informed business decisions.

Market Size and Growth Trends:

Incorporating technologies such as big data, the Internet of Things (IoT), Artificial Intelligence (AI), and others will probably lead to the development of behavioral biometrics services with improved performance. Additionally, the behavioral biometrics market demand is increasing worldwide due to advantages like ease of use, flexibility, security, and efficiency that facilitate integration with cloud solutions. Polaris Market Research conducted a comprehensive research study spanning over [+110] pages, revealing that the global behavioral biometrics market size/share was valued at USD 1,101.33 Million in 2022. The study further indicates that the market will grow at a compound annual growth rate (CAGR) of 25.10% and is projected to touch USD 9,345.99 Million by 2032. Behavioral Biometrics Solution segment is anticipated to witness faster growth in the coming years due to offering advanced analytics and algorithms. Some of the top market leaders are BioCatch, BehavioSec, Plurilock Security Solutions, NuData Security, Bio-Metrica, SecuredTouch, Featurespace, TypingDNA, UnifyID, HYPR & Secured2 and others.

Based on the Application; the Behavioral Biometrics market is sub-segmented into Identity Proofing, Continuous Authentication, Risk & Compliance Management and Fraud Detection & Prevention. The Identity Proofing segment held the largest market share of 40% in 2021. Users with varying levels of privilege are given different authentication alternatives by identity proofing technologies. These technologies also assist in the development of fail-safe procedures for establishing policies for authenticating critical applications. Rising awareness among businesses of the need to protect their data from increasingly complex cyberattacks, malware, identity-related fraud, and data breaches is likely to propel the segment further.

Based on the Deployment; the Behavioral Biometrics market is sub-segmented into On-premise and Cloud. The On-premise segment held the largest market share of 65% in 2021. Internal behavioural biometric solutions are simple to connect and setup with existing internet offerings, which accounts for this. Additionally, on-premises deployment allows for a high level of adaptability for the company, as well as lower expenses in the event that extra resources are required. Based on the End-User, the Behavioral Biometrics market is sub-segmented into BFSI, Retail & E-commerce, Healthcare, Government & Defense, IT & Telecom and Others. The BFSI segment held the largest market share of 28% in 2021. With the increase in fraud and cybercrime, as the customer experience improves, preventing customers from facing risks has become the top issue on the bank's agenda. As new threats appear almost every day, measures must be provided to protect end users from hacker attacks and fraud without compromising the consumer experience. With the rise of fintech start-ups and the upcoming PSD2 (Revised Payment Service Directive) regulations will intensify competition in the industry; customer experience is becoming an increasingly important difference, so a more nuanced approach is required.

5.2 Fully Homomorphic Encryption Market Analysis and Size

In last few years, we have been trusting more of our electronic data to the cloud such as internal company documents, e-mail and personal information. Nowadays, protecting the confidentiality and privacy of that data is a major challenge for practitioners and researchers. Fully homomorphic encryption is one of the most promising approaches which has gathered a lot of attention in last few years. It helps to represent data without giving away access of the data. Homomorphic encryption is extensively used for effective data security. Thus, the data remains safe even in case of a breach.

Data Bridge Market Research analyses that the fully homomorphic encryption market is expected to reach USD 510.06 million by 2030, which was USD 275.57 million in 2022, at a CAGR of 8.00% during the forecast period. In addition to the market insights such as market value, growth rate, market segments, geographical coverage, market players, and market scenario, the market report curated by the Data Bridge Market Research team includes in-depth expert analysis, import/export analysis, pricing analysis, production consumption analysis, and pestle analysis.

Homomorphic encryption is a cryptographic technique that allows computations to be performed on encrypted data without decrypting it. Behavioral biometrics involves using unique patterns and characteristics of human behavior, such as typing patterns or touch gestures, for authentication or identification purposes. Combining these concepts, behavioral biometrics-based homomorphic encryption key generation involves using behavioral data to derive encryption keys for homomorphic encryption schemes. Here are the functional requirements for such a system:

5.3 Functional requirements of behavioral biometrics-based homomorphic encryption key generation

- Capture Data: Acquire behavioral biometrics data from users through appropriate sensors or interfaces (e.g., keyboard, mouse, touchscreen).
- Preprocessing: Process and preprocess the raw behavioral data to extract relevant features or patterns that can be used to generate encryption keys.
- Feature Extraction: Extract meaningful features from the acquired behavioral data to represent the unique patterns associated with each user.
- Pattern Analysis: Analyze behavioral patterns to identify distinctive characteristics and create a reliable representation of the user's behavior.
- Behavioral Biometrics Key Generation: Algorithm Selection: Implement appropriate algorithms and methodologies to transform the extracted behavioral features into a cryptographic key suitable for homomorphic encryption.
- Key Generation Process: Develop a process that utilizes behavioral features to generate encryption keys that are unique to each user and resistant to attacks.
- Homomorphic Encryption Integration: Key Integration: Integrate the generated behavioral biometrics-based encryption keys into the homomorphic encryption scheme for secure data processing.
- Homomorphic Operations: Enable the performance of homomorphic operations using the generated keys while ensuring the confidentiality and integrity of the encrypted data.
- Key Management and Storage: Establish a secure mechanism for storing the generated encryption keys to prevent unauthorized access or tampering.

- Key Revocation and Update: Implement processes for key revocation and periodic updates to enhance security and adapt to changes in user behavior.
- Security: Incorporate appropriate security measures to protect both the behavioral data and the derived encryption keys from unauthorized access, manipulation, or theft.
- Privacy Compliance: Ensure compliance with privacy regulations and standards by implementing privacy-preserving techniques during key generation and storage.
- User Authentication: Integrate the behavioral biometrics-based homomorphic encryption key generation process into authentication systems to authenticate users based on their unique behavioral patterns.
- Verification Process: Develop a verification process that confirms the authenticity of the generated encryption keys and associates them with the respective users
- Performance:
    - Efficiency: Optimize the key generation process to be efficient and not cause significant delays in user authentication or data processing.
    - User Experience: Ensure a seamless and intuitive user experience during the behavioral data collection and encryption key generation processes.
    - Error Detection and Handling: Implement mechanisms to detect and handle errors or anomalies during key generation, ensuring the system remains robust and reliable.
    - Logging and Auditing: Maintain detailed logs of key generation activities for auditing, monitoring, and troubleshooting purposes.
    - Compatibility with Systems: Ensure compatibility with various systems and platforms, allowing for easy integration into existing infrastructure.
    - Scalability: Design the system to handle a growing number of users and adapt to increased data volumes and computational demands.

6 Conclusions

The Deliverable provides an initial look into the market opportunities for technologies developed in the SUSTAIN project. The Deliverable will be used as a baseline for conducting more detailed market analyses per each technology. The follow up work will be reported in D7.2 due M36.