The future of IoT: Expert Survey results

The following paragraphs summarise the main findings of the foresight study on the future of the Internet of Things (IoT) and Ambient Intelligence (AmI). The study was conducted by the Interdisciplinary Center for Technological Analysis and Forecasting at Tel Aviv University (www.ictaf.tau.ac.il) at the end of 2008.

Email invitations were sent to 716 experts. The number of actual respondents was 91 (13%).

The next table shows the level of (self-ranked) expertise of respondents in several IoT technologies. 56% of the respondents consider themselves as experts in general aspects and visions of IoT. The survey respondents have varying levels of expertise in IoT technologies. 41% consider themselves as experts in RFIDs/Sensors, 37% in communications, 32% in IT security, 32% in energy, 20% in software, 19% in identification, and only 15% in privacy. 38% of the respondents are unfamiliar with issues of privacy.

Table 1: Survey respondents' degree of expertise in different IoT technologies

	Unfamiliar	Familiar	Knowledgeable	Expert
General knowledge of IoT	3%	9%	32%	56%
RFIDs/Sensors	3%	20%	36%	41%
Communication	4%	33%	25%	37%
IT security	11%	29%	29%	32%
Energy	8%	35%	25%	32%
Software	18%	41%	22%	20%
Identification	12%	43%	26%	19%
Privacy	38%	37%	9%	15%

Other characteristics of the experts' survey respondents are:

- 37% of the respondents are researchers in a higher education institution, 13% are researchers in government laboratory.
- 17% are managers in private business, 17% are researchers in private business.
- 17% are from Germany, 9% from the UK.

IoT in 2020

The first section of the survey dealt with future visions of IoT/AmI. Respondents were asked to provide their level of agreement to 8 statements that relate to specific scenarios in 2020.

In the first statement, the future scenario refers to a situation where limited connectivity results in relatively small and niche markets for IoT applications (Chart 1). 72% of the respondents disagree with the statement.

The second statement relates to the existence and effectiveness of privacy enhancing technologies (PETs). 62% percent of the respondents agree that PETs will have a mitigating influence on "big brother" fears of possible lack of privacy associated with IoT in 2020 (chart 2).

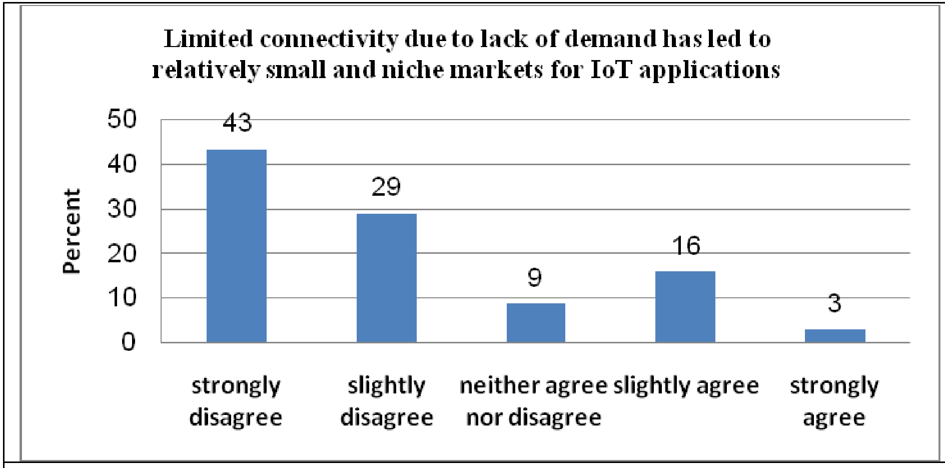

Chart 1: Expert's view on limited connectivity scenario in 2020

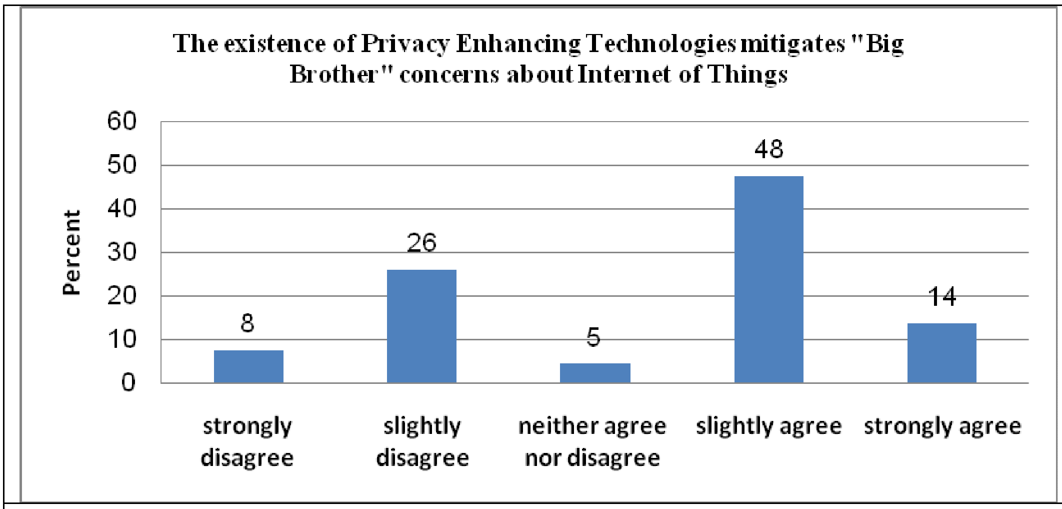

Chart 2: Expert's view on privacy enhancing technologies

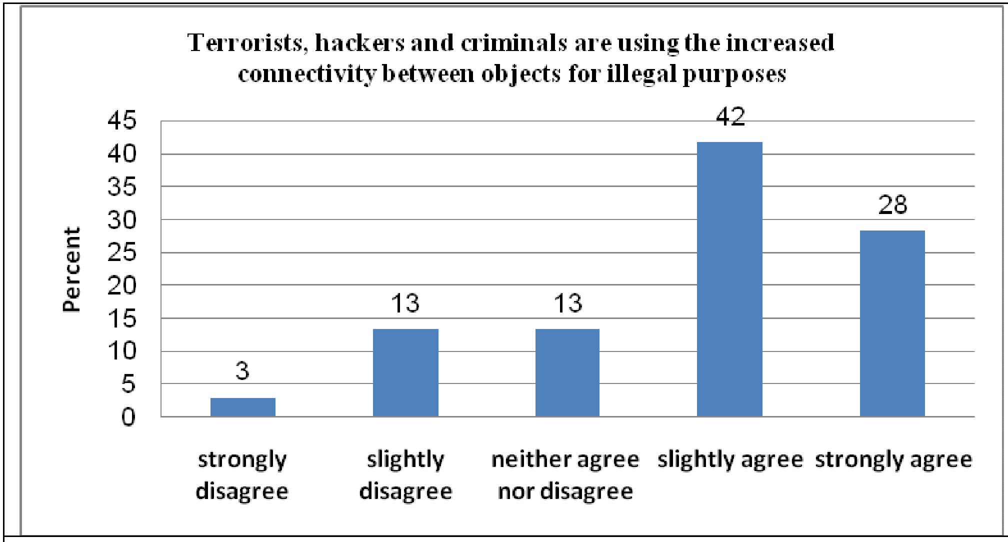

Chart 3: Expert's view on the use of connectivity for illegal purposes

When confronted with a statement claiming that terrorist and hackers can still use increased connectivity in 2020 for illegal purposes, 70% of the respondents agree that this is likely. This seems to conflict with the effectiveness of PETs unless we believe that privacy can be traded against increased benefits of IoT applications (or that the mitigation of "big brother" concerns doesn't necessarily imply elimination/prevention of abuse). The assumption is that users will not be able to fully utilize the benefits of IoT applications without giving up some level of privacy. Indeed, the next chart shows that most respondents (68%) believe that in 2020 people will trade privacy to gain the benefits of IoT applications.

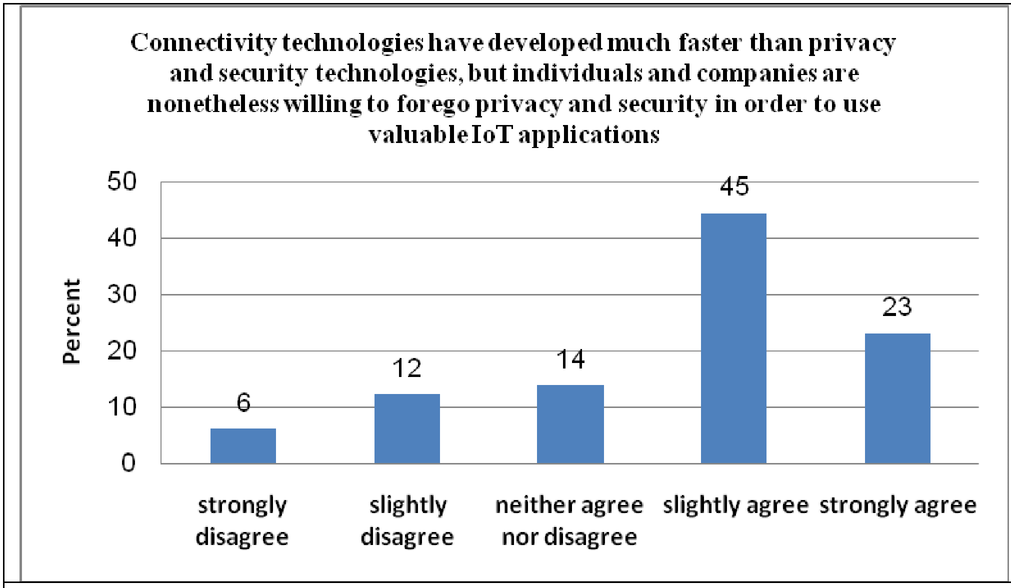

Chart 4: Expert's view on possible trade off between privacy and IoT benefits

A scenario of full scale IoT, where everyday objects and sensor networks are common in workplaces, public places and households is likely to happen in 2020 according to 65% of the respondents (chart 5).

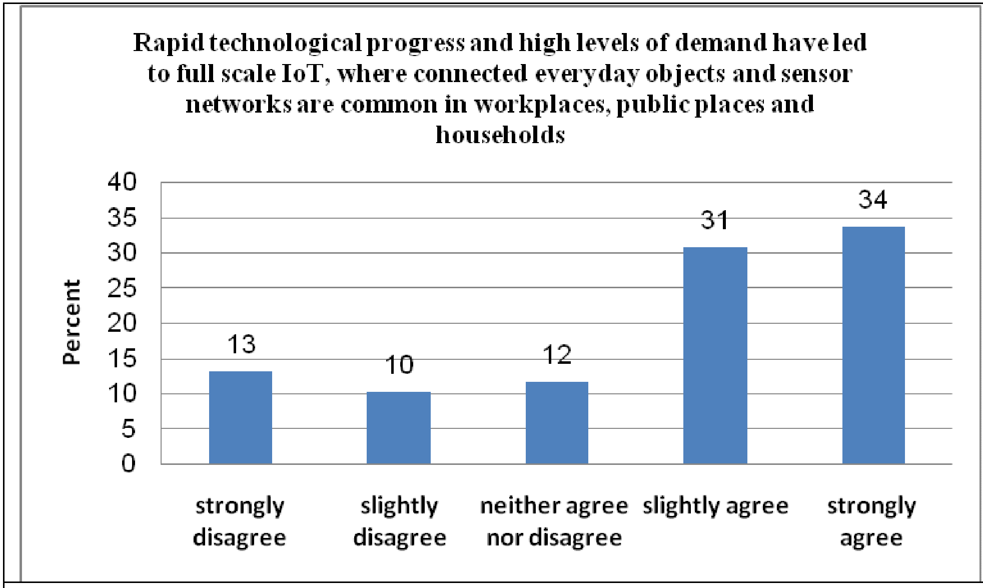

Chart 5: Expert's view on full scale IoT scenario in 2020

The survey respondents were asked to evaluate the possible impact of several factors on the future of IoT on a scale from "very low" to "very high" (1 to 5). The resulting most important factors are clear benefits of IoT applications, cost reduction of hardware components, and governance (chart 6). Privacy and environmental concerns are viewed by the experts as the least important factors. As already implied above (in the explanation to Chart 4), experts do not consider privacy concerns as a major barrier to IoT, since users may trade privacy for beneficial IoT applications. In other words, for users who value an IoT application, privacy concerns are not an issue that will make IoT applications undesirable.

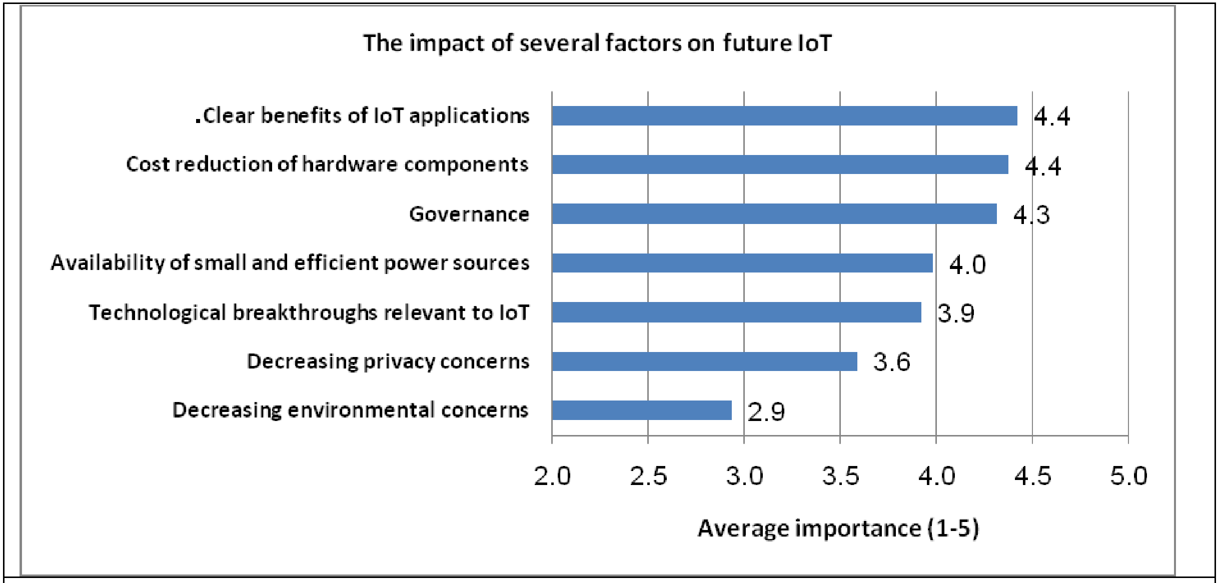

Chart 6: The impact of several factors on the future of IoT

IoT applications

There are several applications that may have a significant contribution to the future market for IoT products and services. The survey respondents were asked to rate the relative contribution of IoT application areas to future market potential (chart 7). The application areas with the highest contribution are logistics, industrial monitoring, the military, healthcare and automotive. Food traceability, PANs, home automation and automatic meter reading will have lower contribution to future potential market.

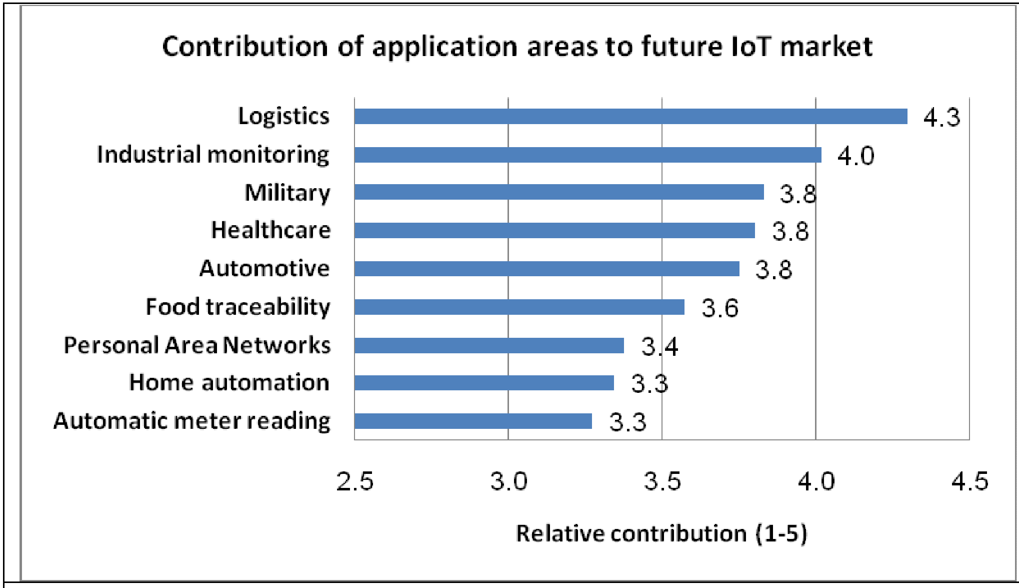

Chart 7: Relative contribution of IoT applications areas

Table 2 describes the assessments of the survey respondents with regards to specific IoT applications. The survey respondents were asked to assess when IoT applications reach widespread use (30% of the target market) and the commercial impact of each application (an estimate of yearly sales).

The application which was rated highest in terms of commercial impact was item-level RFID systems for global tracking and supply chain management. This application is expected to reach widespread use in 2013-2015. The application which was rated 2nd in terms of commercial impact was a global traceability system that covers the majority of goods and enables consumers to trace the origin and preparation characteristics of food products. It is expected to reach widespread use somewhat later – during 2016-2018.

Not far behind, in terms of commercial impact, respondents rated the following applications: Vehicles that are able to autonomously communicate with other vehicles, nationwide incident management system, and personal area networks.

Table 2: IoT applications timing of widespread use and their market potential

	Widespread use*	Sales over $0.75B/y**
Item-level RFID systems for global tracking and supply chain management	2013-2015	81%
A global traceability system that covers the majority of goods enables consumers to trace the origin and preparation characteristics of food products	2016-2018	60%
Vehicles that are able to autonomously communicate with other vehicles, insurance companies, garages and control centers	2013-2015	52%
Nationwide incident management system for the near-real-time detection, identification, and assessment of chemical, biological, radiological, nuclear, and explosive threats.	2019-2020	38%
Personal area sensor networks embedded in clothes, cellular phones and/or inside the body	2016-2018	38%
"Smart dust" for information acquisition in various applications (military, environment…)	2016-2018	38%
Large-scale distributed sensor-rich wireless networks designed to track multiple moving objects such as vehicles or animals	2016-2018	33%
** Percent of respondents assessing yearly sales of over $0.75B * Period when the application reaches 30% penetration of target market (based on the mean of experts estimates)		

IoT technologies

RFID & sensors

In these technology areas, experts addressed 7 specific technologies (see Table 3). The market potential of the technologies varies and so are the periods where they are expected to reach widespread use. Biodegradable sensing devices that can be organically decomposed after completing their function, will only reach widespread use in 2019-2020. On the other hand, active RFID tags that cost less than 1 dollar are expected to reach widespread use much earlier, in 2013-2015. Context-aware sensors that are able to process information from their surrounding, from other sensors, and from users, are an important element in future IoT applications. This technology is expected to reach widespread use in 2016-2018.

Table 3: RFID/Sensors technologies timing and market potential

	Widespread use*	Sales over $0.75B/y**
Chipless tags that enable printing directly on the product's surface	2016-2018	58%
RFID active tags that cost less than 1$	2013-2015	57%
Biodegradable sensing devices	2019-2020	53%
Microprocessor based sensors	2016-2018	52%
Context aware sensors that are able to process information from their surrounding, from other sensors, and from users	2016-2018	48%
Wireless Sensor Networks connecting multitude of sensors	2016-2018	47%
Multimodal sensing systems enabling complex applications such as implants monitoring vital signs inside the body	2019-2020	45%
** Percent of respondents assessing yearly sales of over $0.75B * Period when application reach 30% penetration of target market		

Personal identification & authentication

The largest market potential in this area is associated with a technology to manage the identity of a huge number of constantly emerging and disappearing objects – a feature necessary for large-scale IoT, in which the IT industry is not experienced yet. Today there are several objects ID technologies and standards, which present a barrier on the road to full scale IoT. Facial and vocal recognition system with 99.9% accuracy are expected to become widespread use also in 2016-2018, and DNA recognition will become widespread use only in 2019-2020, given the cultural and ethical issues that have to be resolved by then.

Table 4: Personal identification & authentication technologies timing and market potential

	Widespread use*	Sales over $0.75B/y**
Technology to manage the identity (ID) of a huge number of constantly emerging or disappearing objects	2016-2018	63%
Personal identities authenticated with Match-on-card biometrics	2016-2018	49%
Facial and vocal recognition system with 99.9% accuracy	2016-2018	46%
Intelligent agents for networking personal information	2016-2018	42%
DNA recognition	2019-2020[1]	35%
** Percent of respondents assessing yearly sales of over $0.75B * Period when application reach 30% penetration of target market		

[1] The standard deviation here is higher than average due to disagreement between experts on the period of widespread use. Additionally, 20% of the respondents said that widespread use will never be reached (Appendix 1).

Communications

All of the communications technologies included in the survey will reach widespread use towards 2013-2015.

Table 5: Communication technologies timing and market potential

	Widespread use*	Sales over $0.75B/y**
Mesh networks consisting only of mobile devices	2013-2015	63%
A system that allows ad hoc communication between wireless information terminals	2013-2015	53%
NFC enabling individuals to transact with RFID tags	2013-2015	50%
ZigBee for networking very large number of sensors	2013-2015	44%
6LoWPAN for IP communications over IEEE 802.15 based networks	2013-2015	36%
UWB for sensor networks	2013-2015	28%
** Percent of respondents assessing yearly sales of over $0.75B * Period when application reach 30% penetration of target market		

Privacy & security

The technologies that were included in the survey in the area of privacy & security are varied in timings of widespread use. Anonymous web surfing and anonymous credentials transactions will reach widespread use earlier, around 2010-2012. RFID with privacy control and revocable biometrics will reach widespread use later, in 2013-2015 and 2016-2018. Widespread use of quantum cryptography will arrive towards the end of the decade. Non-linkable digital payment for disguising digital transactions seems to have the highest market potential.

It should be mentioned that a relatively large percentage of the respondents (around 20%[2]) assessed that some of the technologies in this area will never reach widespread use. It is possible that some experts do not believe in the massive use of privacy technologies in the world of IoT.

[2] The percentage figures in the tables and charts do not include respondents who said that widespread use will never be reached or respondents that did not know the answer to the question.

Table 6: Privacy & security technologies timing and market potential

	Widespread use*	Sales over $0.75B/y**
Non-linkable digital payment for disguising digital transactions	2016-2018	57%
Anonymous web surfing for maintaining privacy in online activities	2010-2012	55%
Secure communications using quantum cryptography	2019-2020[3]	50%
A publicly available algorithm with theoretically proven safety concerning the prevention of digital watermark removal.	2013-2015	48%
Anonymous credentials assisting users with conducting private online transactions	2013-2015	47%
RFID with privacy control	2013-2015	45%
Private and revocable biometrics enabling users to be the sole owners of their biometric identity	2016-2018	44%

** Percent of respondents assessing yearly sales of over $0.75B
* Period when application reach 30% penetration of target market

Power sources

Power supply technologies in the survey included energy harvesting technologies (solar, vibration, piezoceramic), and other technologies, such as printed batteries and wireless power supply. Table 7 presents the year of widespread use and market potential of the various technologies. For energy harvesting technologies, solar energy precedes vibration and piezoceramic devices in time, and also has higher market potential. Ultra low power chip sets and RFIDs with battery life of 10 years will reach widespread use around 2016-2018 with relatively higher market potential. Wireless power supply will also reach widespread use later, around 2016-2018.

Table 7: Power supply technologies timing and market potential

	Widespread use*	Sales over $0.75B/y**
Ultra low power chip sets for RFID and sensors	2016-2018	64%
Wireless power supply to sensors	2016-2018[4]	59%
Solar cells for energy harvesting	2013-2015	58%
RFID tags with battery life of 10 years	2016-2018	56%
Printed batteries manufactured with sensors	2016-2018	53%
Vibration devices for energy harvesting[5]	2016-2018	48%
Piezoceramic device for energy harvesting	2016-2018	32%

** Percent of respondents assessing yearly sales of over $0.75B
* Period when application reach 30% penetration of target market

[3] The standard deviation here is higher than average due to disagreement between experts on the period of widespread use

[4] The standard deviation here is higher than average due to disagreement between experts on the period of widespread use

[5] The standard deviation here is higher than average due to disagreement between experts on the period of widespread use

Software for IoT

Software technologies for IoT are needed to provide intelligence to future applications. IoT P2P (for data exchange and information dissemination) is expected to reach widespread use around 2013-2015. IoT service composition (several devices combining to offer richer services) is expected to reach widespread use later, around 2015 with higher market potential. Collective intelligence and intelligent spontaneous services will arrive later, around 2016-2018, and local comprehensive AmI around 2019-2020 with the lowest market potential.

Table 8: Software technologies timing and market potential

	Widespread use*	Sales over $0.75B/y**
IoT service composition (several devices combining to offer richer services)	2016-2018	51%
Collective intelligence (a large number of devices working together invisibly for the benefit of users) - Technological Realization	2016-2018[6]	51%
Intelligent spontaneous services (devices offering relevant services at the right time by observing their environment)	2016-2018[7]	50%
IoT P2P (for data exchange, information dissemination)	2013-2015	44%
Local comprehensive AmI (intelligent environments capable of predicting users needs)	2019-2020[8]	39%
** Percent of respondents assessing yearly sales of over $0.75B * Period when application reach 30% penetration of target market		

The most important software related domain, in terms of contribution to AmI/IoT, is embedded systems, followed by distributed systems, complex system design and human-machine interface (chart 8).

[6] The standard deviation here is higher than average due to disagreement between experts on the period of widespread use

[7] The standard deviation here is higher than average due to disagreement between experts on the period of widespread use

[8] The standard deviation here is higher than average due to disagreement between experts on the period of widespread use

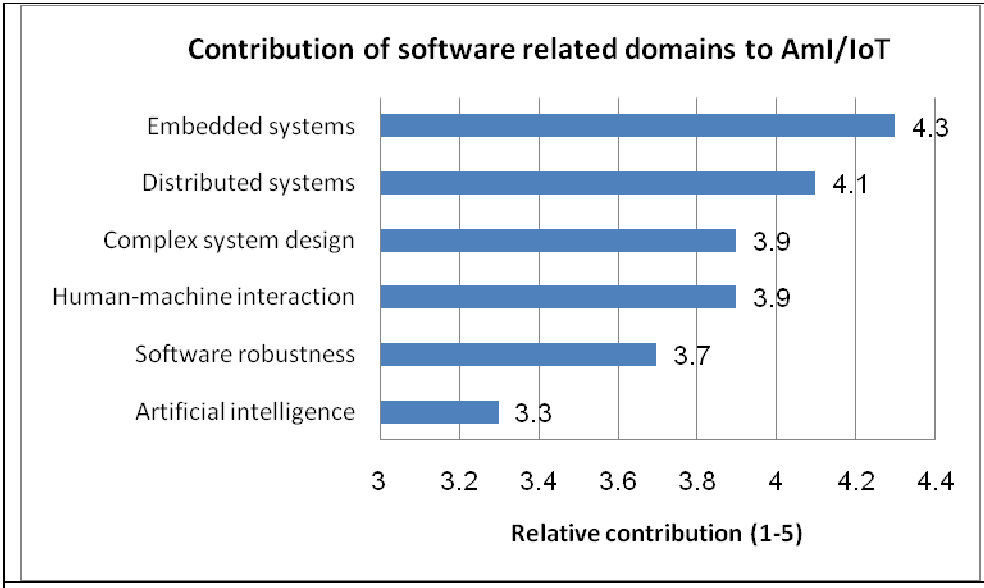

Chart 8: Software technologies contribution to AmI/IoT

Technology challenges

The experts were asked to rate various technology challenges by their contribution to the realization of the AmI/IoT vision (chart 9). Extending battery life[9] was rated first, followed by enhancing data security, enhancing data privacy, miniaturizing hardware components and developing self-adaptive software.

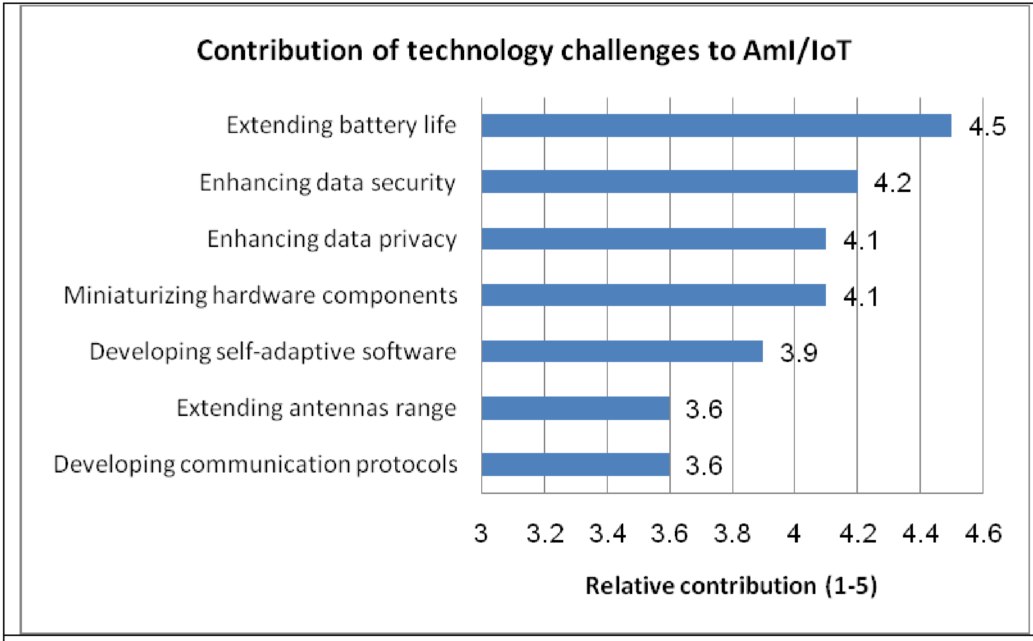

Chart 9: Technology challenges contribution to AmI/IoT

[9] This may be interpreted as long-endurance power sources in general (including energy-harvesters) and not only batteries

About ICTAF

Founded in 1971, ICTAF is a leading institute in Technology Forecasting, Foresight, Assessment and Roadmapping. ICTAF is involved in strategic and long-term planning and is very active in the international community. It taps the expertise of world-class scientists at Tel Aviv University and other well-known research establishments to create a core body of knowledge in diverse fields.

ICTAF functions as a think-tank, working alongside its government and business clients to produce far-reaching conclusions that draw from a unique blend of academic research and market know-how.

ICTAF's Mission is:

- To help policy-makers reach informed decisions based on technology's role in the development of economy and society.
- To serve as a think-tank for future policy planning in Israel and abroad.
- To harness the knowledge of Tel Aviv University's scientists and scholars for the benefit of the economy and society.
- To enhance its leadership in multidisciplinary foresight - covering science, technology, economics and society.

Contact persons:

Dr. Yoel Raban, Senior Researcher	raban@post.tau.ac.il
Dr. Aharon Hauptman, Senior Researcher	haupt@post.tau.ac.il
Dr. Yair Sharan, Director	sharany@post.tau.ac.il