Future Security Challenges for Smart Societies: Overview from Technical and Societal Perspectives

Mohammad Aldabbas
International institute of management in technology (iimt)
University of Fribourg
Fribourg, Switzerland
e-mail: mohammad.aldabbas@unifr.ch

Xuan Xie
School of Automation Engineering
University of Electronic Science and Technology of China (UESTC)
Chengdu, China
e-mail: xiexuan@uestc.edu.cn

Bernd Teufel
International institute of management in technology (iimt)
University of Fribourg
Fribourg, Switzerland
e-mail: bernd.teufel@unifr.ch

Stephanie Teufel
International institute of management in technology (iimt)
University of Fribourg
Fribourg, Switzerland
e-mail: stephanie.teufel@unifr.ch

Abstract—**Human societies went through a long journey from fundamental Society 1.0 to smart Society 5.0. From a security point of view, each phase of development has its characteristics and specialisation. In modern research, when considering security matters, the focus cannot be only on technology but also society, as a group of human beings, needs a different perspective. Rapid technological development brings higher standards and quality of life, while our security standards and personal perceptions of security concepts need to adapt and follow the pace of these developments. This paper stimulates a new concept of societal security, along with a review of various kinds of threats to Society 5.0. The main objective of the paper is to shed light on the risks and threats facing future societies. Related to the here and now, it points out where interdisciplinary research is indispensable and still needs to be done to find answers and solutions. However, the originality of this paper lies in the fact that it combines both the technical and societal perspectives.**

Keywords-societal security, smart, 4th industrial revolution (4IR), society 5.0, smart society

I. FROM FLINTS TO ARTIFICIAL INTELLIGENCE

The history of humankind reaches a long way into the past - according to some ecologists [1] approximately 2 million years. However, cultural evolution started to emerge only 30'000 years ago, when, for the first time since the dawn of humanity, humans witnessed the birth of the first society.

The very simple hunter-gatherer nomads' society is considered as Society 1.0. This form of society lasted for around 20 millenniums. People in this society used simple tools, and for subsistence depended mainly on foods gathered in the wilderness. They moved from one habitat to another over the year. The primary motivator for such mobility was the availability of the resources in their environment [2].

Technology advances and demographical changes, together with developed social structure and organisation, transformed hunter-gatherer society into a more settled society [3]. First signs of the cultivation of wheat and barley and hand-made pottery were discovered in Mesopotamia [1], declaring the birth of Society 2.0, also known as the Agrarian society.

Significant milestones for the humanity took place in the very dominating and long-lasting Agrarian society, such as the start of the Bronze Age, the invention of the first alphabet, building pyramids, and the birth of Renaissance.

By the end of the 18th century, the discovery of laws of gravity, the birth of modern physics, and then the invention of steam engines triggered the Industrial Revolution, which radically changed the face of the Earth forever. The industrial revolution is considered one of the most critical developments in the history of humanity that shaped the contemporary world on every level [4]. The impact was extensive and not only limited to family relations, transportation, environment, society, and other.

The first industrial revolution depended on production using steam power, water, and coal. It started roughly around 1784 and lasted until 1870 when the second industrial revolution arrived with the invention of electricity, which allowed mass production.

In this era, the use of petrol and steel radically increased, following the invention of the first automobiles. This phase lasted until the third industrial revolution in 1969 – a digital revolution. From 1969 many European universities started offering computer science courses, while at the same time in the U.S. the predecessors of the Internet started. The first Programmable Logic Controller (PLC) was also introduced at about the same time. The new digital and IT systems

978-1-7281-5736-8/20/$31.00 ©2020 IEEE

advanced production processes through the further introduction of automation. The emergence of the internet and modern communication systems propelled the globalisation as we know it today.

While the used terminology in the west did not change for post years, on the other side of the planet, appeared what is known as Society 4.0: The Information Society.

The information society was initially developed as a national plan in Japan in 1972. Japan's Information Society aimed to embark into the new era after the post-industrial revolution by the year 1985 [5] and to promote and prosper human intellectual creativity, where the production of information values is the driver for the transition and development of society.

The most recent significant development in the era of the Industrial Revolution is the fourth industrial revolution, also known as 4IR. Initially, it was a strategic initiative of the German government to lead digital transformation in 2011 [6]. Around the same time, the USA had a similar lesser-known initiative focusing on the future of manufacturing [7].

The impact of 4IR affects many aspects, including the whole value chain, society, environment, smart objects [8] and many more.

Shortly after the introduction of 4IR in Germany, the concept gained recognition, got accepted, and adopted worldwide. It shifted from the first application area in manufacturing to other domains such as education and logistics [6]. Note that in some literature, 4IR is referred to as Industry 4.0. However, this concept remains unclear in the literature [8].

One of the side-effects of the developments of these stages of the Industrial Revolution is the issue of "ageing society". Especially Japan is an ageing nation that at the same time suffers from a sub-replacement fertility rate. These trends lead to a demographic change that will shape the future of the country [9]. In response, the government launched an initiative to accelerate the transition to Society 5.0 [10], the super-smart, human-centred society that aims to improve the quality of life for all individuals while increasing the roles of robots, to overcome the restriction in natural and human resources.

Fig. 1 shows a brief history of human societies since the dawn of the first recognised society.

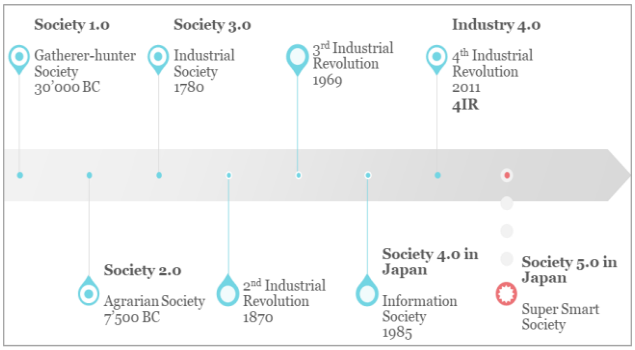

Figure 1. History of human societies.

The digital transformation of society based on sensors and information and communication technologies (SICT) is a dominant force that has shaped society since the 1980s, i.e. from Society 4.0 onwards. It holds a multitude of challenges resulting from the speed, range and influence on different aspects of modern life. There are benefits for the public at large that are beyond our wildest expectations, e.g. a variety of communication, cooperation and participation possibilities. A future "super-smart" society will not be shaped by lone fighters, but by the interaction of groups of people, the so-called crowds. In this context, the term crowd takes on a new dimension and develops into a concept through the scope of the ubiquitous availability of sensors, i.e. data, and information and communication technology (ICT). Crowds will pool their resources through ICT to achieve optimal efficiency and effectiveness in achieving progress and well-being [11].

Based on the research of Mark Wexler [12], who showed the development of the meaning of the term Crowd from a social problem to a problem solver, the work of Teufel and Teufel [11] took this further and described the Crowd as an enabler of a smart society. The Crowd Principle is defined as the collective effort of individuals or profit or non-profit organisations, or both, pooling their resources through SICT applications to improve sustainable well-being (both by and for the community) [11].

So far, so good. If we apply the crowd principle specifically to the energy sector, then "*pooling resources through SICT applications*" can mean, for example, the widespread use of smart meters and thus the establishment of a smart grid, which in turn allows energy to be used more efficiently depending on consumption. This, in turn, is beneficial to the "*improve sustainable well-being*" aspect. However, it should be noted that for this purpose data such as consumption, generation and feed-in data must be collected and processed. This allows conclusions to be drawn about the extent, type and period of energy consumption of persons living in a household, i.e. it is person-related data.

The data generated by smart metering is critical, as it makes it possible to generate user profiles of individual persons. Based on the electricity consumption, which is precisely monitored by smart meters, it is possible to show in detail when a consumer goes to work, when they are away from home, how and when they prepare their meals, or when and how often they use other household appliances. All of this is virtually invisible for the persons concerned since the systems collect the data continuously and autonomously.

This example shows that a smart society cannot be defined solely based on digital technologies. Even if crowds take on the role of enablers according to the defined principle, it is clear that, in addition to the financial and economic framework conditions, it is necessary to have the political framework and responsible cross-sector acting above all. The inter-sectoral linking of data and processes, while respecting people's privacy, creates smart solutions that lead to added value for society on a social, economic and ecological level and thus makes sustainable well-being [13] possible. We speak of a smart society.

II. Challenges of a Smart Society

When talking about challenges and difficulties for the future society, it is absolutely essential to realize that a smart society is a socio-technical system [13]. It is therefore not sufficient to consider just technical aspects, but social characteristics must also be taken into account.

A. Social Science Perspective

A smart society is as vulnerable as any other society. However, the mechanism of this vulnerability is different since the characteristics and properties of this society are unique. The problem here is that Society 5.0 is not exempt from the usual risks and threats that transpire in conventional society. On the contrary, a smart society is somewhat open to additional types of risk. Some kinds of threats seem similar to the ones faced in conventional society; however, their unique characteristics and features classify them as the new risks and threats that come with the smart society.

The authors present the threats from a societal perspective [11], [14], [15], as well as from a technical perspective, such as:

- New technologies carry with them new varieties of addictions, such as the internet and online gaming addiction. Studies showed that many users have internet gaming disorder [15].
- Digitalisation and excessive use of robots are claimed by many scholars to generate new jobs for humans. However, the loss of jobs that are taken by these robots is considerably more significant.
- In cyberspaces like twitter, one misunderstood tweet can have severe irreversible impacts on the lives of the victims. The massive power of social media presents some potential danger.

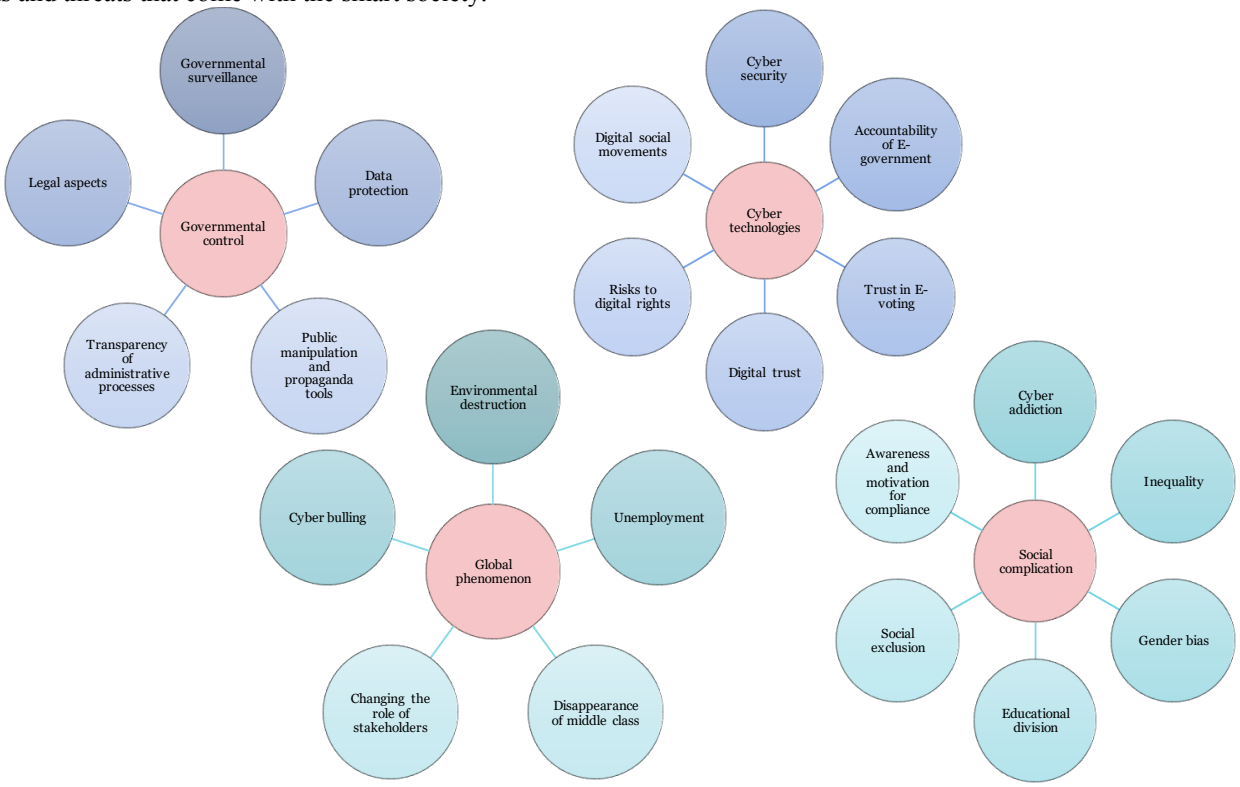

Figure 2. Risks and concerns for smart societies.

Fig. 2 shows some of the risks.

The risks and threats mentioned above raise questions that need answering:

- Should we apply all the technology that we can apply?
- How far should the technology be applied? Where is the limit?
- Will Society 5.0 lead into a profit-oriented authoritarian society?
- Technology vs Humans: Who is in the driver's seat?
- Are there rights and ethics for robots?

B. Aspects of Security from a Societal Perspective

Based on the cause research has identified two categories of risk factors: technical and human factors [16]. Likewise, it is possible to address security matters from two perspectives according to the target: societal perspective and technical perspective. However, generally speaking, the authors will first present a general overview of the risk factors, from

which every society should be protected. Later the authors will discuss the technical aspect in more detail.

Brooks examined two issues to define the knowledge fields of security: the knowledge categories and subordinate concepts of security, and the possibility to develop a security science framework [17]. Based on his research, Brooks defined 13 core categories of security.

- Criminology
- Business continuity management
- Fire and life safety
- Facility management
- Industrial security
- Information and computing
- Investigations
- Physical security
- Safety
- Security law
- Security risk management
- Security management
- Security technology

Therefore, it can be stated that security encompasses a vast range of different bodies of knowledge. Changes in the economy and society influence the relevance of the individual bodies. Undoubtedly, advancing digitalisation ensures that the core category information and computing, in particular, are becoming increasingly important.

C. Technical Perspective

The base of the smart society is data. The whole life-cycle of data includes at least five processes: collection, communications, storage, usage, and destruction. These processes are not linear, as they can partially overlap, as shown in Fig. 3. Most applications, such as smart home, smart grid, telemedicine, and smart transportation, incorporate the whole life-cycle of data. Technologies, such as the Internet of things (IoT), cloud calculation, artificial intelligence (AI), have a deep fusion with part(s) of the life-cycle of data.

Every wave of technology adoption has its challenges, and smart society technologies are no exception to the rule. Throughout the entire life-cycle of data, we are facing many hurdles, such as privacy protection, power consumption, bio-compatibility, and data fusion. The following shows some critical challenges from the technical perspective.

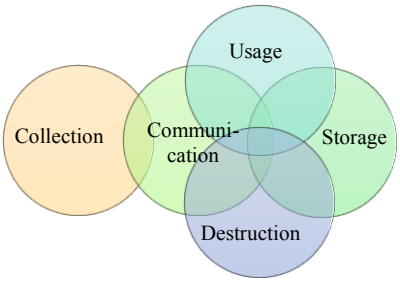

Figure 3. Life-cycle of data.

1) *Efficiency*: in the smart society, IoT, wireless body area network (WBAN), the industrial Internet of Things (IIOT), and mass data are a standard. However, all resources, including battery power, communications bandwidth, memory storage, and computation capability, are limited. So "efficiency" becomes one of the very significant challenges.

More and more researchers are looking into it. The methods work on different levels, and even cross-levels are used to achieve higher energy, communication, and computation efficiency. Previous research improved the design of physical and medium access control (MAC) layers with an efficient hop system or adaptive duty cycle to improve the energy efficiency for WBAN [18], [19]. Furthermore, in recent years, fog computing, edge computing, context awareness, cellular communications, game-theory based energy management approach, are employed to achieve higher efficiency [20]-[24]. A scalable IoT architecture based on transparent computing is proposed, which is used in the scalable, lightweight wearables to obtain better energy efficiency as well as contextual information processing [25]. Liu *et al*. proposed an effective knowledge-aware proactive node selection (KPNS) system to achieve both energy efficiency and high monitoring performance [26]. Although researchers have tried many methods to achieve higher efficiency, the efficiency issue is still a challenging area considering the increasing amount of data.

2) *Data Heterogeneousness:* In the smart society, data and communication protocols are both heterogeneous. This is another crucial challenge that affects almost every process in the whole life-cycle of data, especially when considering large-scale heterogeneous data traffic, awareness, access, and mining. The collected data is of different resolutions, accuracy, and reliability [27]. Not only the types of data are heterogeneous, but so are the requirements. Some are real-time data, while others are more time-resistant. Processing multi-type and multi-requirement data incurrs high computation and communication costs, which, in return, also, affects energy consumption and hardware costs. The internal-confidence degree, external-confidence degree, and data utility are used to evaluate the reliability of the data sources [28],[29]. Structural analysis and deep-learning-based approaches are increasingly utilised for attracting adequate information from the big data in the heterogeneous information networks [30],[31]. However, the open issue is

how to select the source best and optimally arrange the data processing.

MAC layer protocols play an essential role in supporting heterogeneous sensors (devices) and different networks [32]. However, it is unavoidable that the heterogeneousness will also lead to the issue of interference and coexistence. Some works have studied the interference and coexistence between different networks, including IEEE 802.15.6, ZigBee, WiFi, 5G, radar, etc. [33]-[36]. In [37] and [38] it was shown that the ZigBee network (operating at 2.4 GHz) might be subject to the interference issues with networks based on IEEE 802.15.6, Bluetooth, and WiFi. Furthermore, IEEE 802.15.6, which is commonly used in WBAN supports 10 WBANs for a space of 6m×6m×6m and at the most maximum of 256 nodes per body. This will present an increasing challenge as society increases the usage of sensors over time.

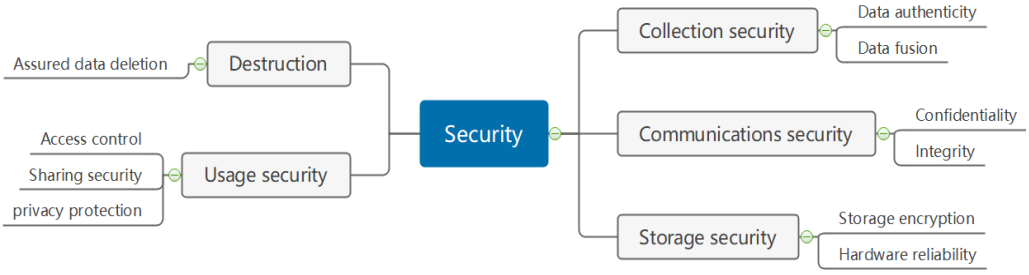

Figure 4. Challenging aspects of security from the technical perspective.

3) *Hardware environment compatibility:* In the smart society, sensors will be more and more commonly used, so environment compatibility becomes increasingly essential, especially in the domain of smart health. For different purposes and environments, the hardware design, such as the size, shape (form), materials, life, implant location, should be considered comprehensively together with the environmental compatibility, such as bio-compatibility [32], and performance of communication. This will present challenges for hardware design, especially the antenna design. At the same time, this crucial issue drives the development of innovative materials, such as flexible electronic materials. The design constraints based on the locations and organs were discussed in [39]-[41]. Moreover, the electric and magnetic energy absorbed by human tissues might lead to overheating issues and result in damage to human tissues, as more and more wearable and implant sensors will be used, and as such should not be overlooked [42]. From this perspective, the absorption ratio was reviewed in [43] and proposed some temperature aware routing algorithms to mitigate this issue. In regards to this point, ultra-wideband (UWB) technologies are attracting increasing interest.

4) *Security, privacy, and trust*: As the development of smart information technologies continues, such as cloud computing, fog computing, and context awareness technologies, the issues of security, privacy, the trust becomes a critical factor that even implicitly hinders the adoption and growth of smart society. The security and privacy challenges concern all aspects of the data life-cycle, including access control, policy enforcement, secure middleware, authentication, computing algorithms, [44]-[46]. Trust is a very complex concept, whose meaning is varying according to different contexts. Some researchers proposed that it is associated with the source reputation, the behaviour of the source, and users' expectations [47]-[49]. It can be concluded that, although trust is a complex notion, at the base of it lies security and privacy protection.

For the security issues, in the life-cycle of data, we have to pay more attention to the following aspects, as shown in Fig. 4. In the smart society, the data have the following features: massive, multi-sourcing, heterogeneous, and sparse [27], [50], [51]. So, for the collection process, data authenticity and data fusion are the most challenging aspects [51]-[54]. In the communication aspect, confidentiality and integrity concerns are highly associated with security. Currently, encryption technologies, such as homomorphic encryption technology, are commonly used method to ensure data security in data communication and storage. However, with the emergence of quantum computing, traditional encryption methods, and even blockchain technology, are challenged by the computing ability of it [55]. Furthermore, disk storage reliability is also an important aspect of data storage security. The trusted solid-state disk (TrustedSSD) technique is becoming a potential technique in the storage security field [56]. In the usage process, access control, sharing security, and privacy protection are three aspects worthy of more attention. Traditional access control methods are confronting serious challenges in authorisation management, fine-grained control, privacy protection, implementation architecture [57]. For sharing security, although we lack global security standards, there is no shortage of references which are working on the sharing security. Attribute-based information flow control [58], game-theoretic information flow control [59], attribute-based encryption [60], blockchain-based methods, etc. are proposed. Privacy protection methods include *k*-anonymity, *t*-closeness, *l*-diversity, and graph-based methods, and many more. The conflict of privacy protection and data analysis becomes obvious [61].

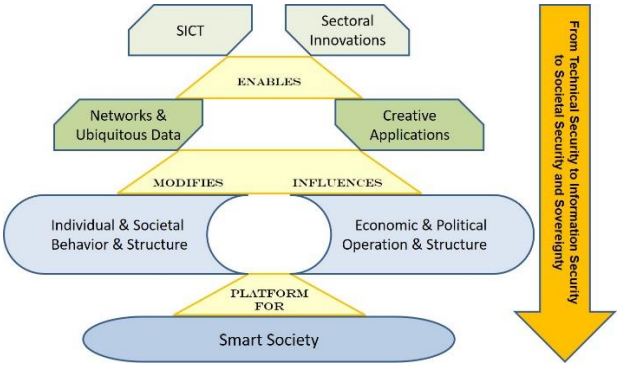

Figure 5. Smart society conceptual framework, based on [11]

Moreover, the popularity and development of social media provides potential attackers with abundant resources from which they can try to derive users' privacy and relationship details based on the users' social media data. So the research on social media anonymity becomes another area of increased interest. Within the cloud computing environment, personal data is usually cached, copied, and stored by the third-party — the user loses the full control right for all the copies of their data. Thus, assured data deletion is also a crucial challenge in the data life-cycle, which is becoming another research hot spot [62],[63].

III. The Evolvement of Societal Security

A future smart society can be envisioned as a conglomerate of digital technology and bottom-up consortia of individuals embedded in corresponding social and political-economic structures, as shown in Fig. 5 [11].

The networking of people and things, the permanent collection and availability of data, artificial intelligence and deep learning are the results of achievements and innovations in science and technology, and they stimulate a radical change in society and the economy [64]. Even if digitalisation seems to simplify and facilitate specific processes, complexity is growing at all levels [10]. The networking of things as well as of people and things leads to unprecedented challenges for society; this applies in particular to security.

When we have talked about security so far, it has often been a selective matter, meaning that the focus has been on a single object and has been more reactive than proactive (reaction/action). The networked digital world of a smart society redefines the complexity of security, which must be viewed multidimensionally. Let us, for example, look at the mobility aspect of an individual in smart society, as shown in Fig. 6 [65].

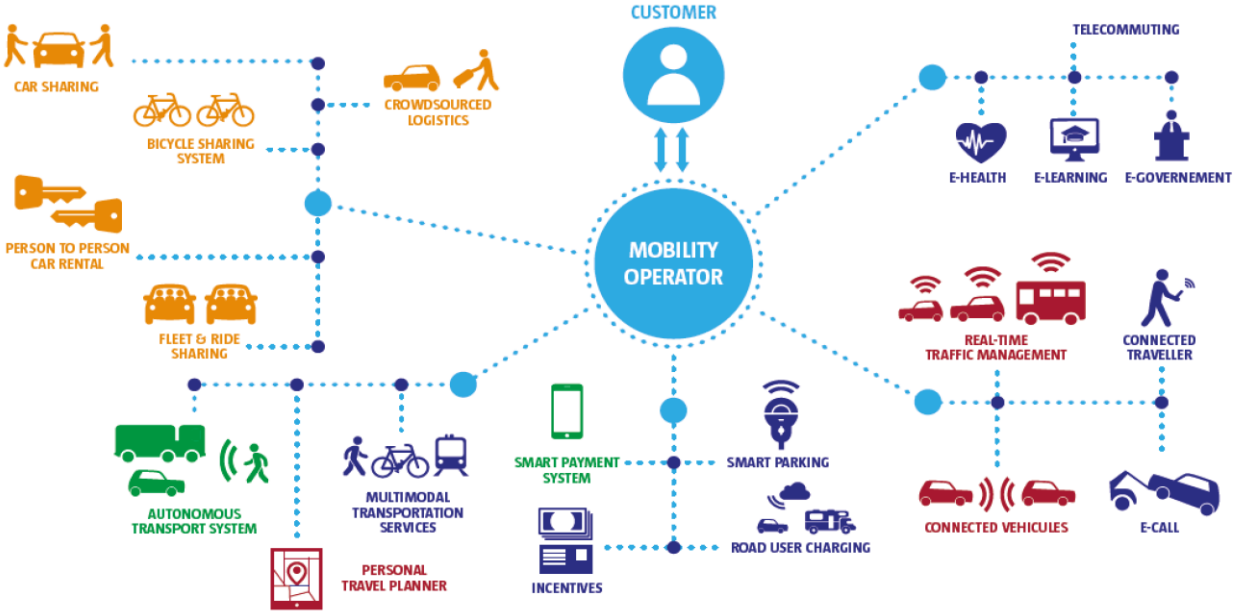

Figure 6. Mobility aspects of an individual in a smart society [65].

The individuals will, of course, fulfil their mobility demands multimodally and be mostly dependent on SICT. For a security assessment regarding a journey from A to B, the following factors should be considered:

- Intermodality - ensuring connections and reliable information
- Smart Payment - secure payment process and privacy
- Road Charging - secure payment process and privacy
- Autonomous Transport System - secure SICT and ethical programming

- Connected Vehicles - secure communication and ethical programming
- E-Health - privacy for informational self-determination, transparency in terms of user profiles
- Etc.

This enumeration only provides a glimpse into the security complex for a journey from A to B.

The rapid technological changes that accompany us in our daily life implies two things. First: the standard and quality of life are increasing. Second: our standards of security and personal perception of the new notion of security should at least attempt to match the pace of these changes. Therefore, the societal security has to be dynamic and comprehensive to comprise these changes and challenges, so that it can provide with an acceptable level of protection. Nonetheless, in the new perspective, societal security attempts to cover all concerns of all individuals that are coupled with technological advance and societal revolution whether in 4IR or Society 5.0

Societal security has a diverse perspective for the mentioned security concern above. For example, an individual cares about her safety, job, privacy, and prosperity. She is willing to take care of her needs and strive for her safety, but there are limitations to what she is able and willing to do. Moreover, she is not able of being up to date with all the rapid digital and technological changes that never slows down, which is a big concern for her. This example shows the importance of someone stepping up and taking over the responsibility of preserving society's safety and prosperity.

It is necessary to change the understanding and adjust the perspective in order to adopt the unique security characteristics of the smart society. For instance, the society and economy will be considerably impacted by 4IR as more than 30% of people use social networks to connect, learn and exchange information. As customers, they are also getting more involved in production and distribution chains [66]. Consequently, failing to change the notion of security will leave all individuals very exposed and vulnerable to severe and sometimes unexpected consequences.

Furthermore, in the future smart society, ethical research will become more critical in societies with advanced technologies as it is essential to understand the unique nature of the smart society. The digital revolution will change our views about many principles and values, and the priorities of these values [67].

Today's tools and equipment for societal security show signs of apparent failure. Most notable examples are an economic crisis, environmental concerns, data protection, privacy, internet surveillance, digital ethics and much more. All these are subjects that appear very often in the news; however, not in a desirable positive way. For example, IoT systems today do not adequately achieve the desired functional requirements and cannot reach the ultimate security and prevent privacy risks. Additionally, attacks on cyber-physical systems could result in physical damage and even endanger human life [68].

Now, imagining how the future will look like, assuming that these unsolved problems get even more complex, the tension between *sustainable well-being* and the *inherent risks* becomes obvious. In order to be able to respond to future challenges, we need social security equipped with modern tools and methods. The power to control and introduce changes must be done responsibly and with a lot of considerations. In other words, society needs smart sovereigns.

IV. Implication

Learnings from the importance of societal security are that there are barely any tools to protect us, as individuals, from the incoming wave of digitalisation and that we are by no means ready for such transition in terms of ability to react to threats. More importantly, people are not aware enough of the alarming implications of what is coming.

This paper is the motivation for further research to examine the impact of risks and threats on smart societies. Next step will be sketching a new method and a way of control, which ensures that the crowds are the true sovereigns. They have control over the security of their smart society and the power to intervene to prevent technology developers from exploiting the weaknesses and flaws within society. The primary intention of developing the new approach is to create a roadmap, which facilitates the path to a smart society in a manner that assures the sustainable well-being of all individuals [13], with the emphasis on crowds as enablers [11]. Future work will address this novel concept in detail to contribute to a better understanding and development of tools to reduce the risks and threats in smart societies.

Acknowledgement

This work was funded by the Canton of Fribourg, Switzerland, through the Smart Living Lab project at the University of Fribourg. Furthermore, it was partly financially supported by the National Natural Science Foundation of China under Grand No. 61701095.

References

[1] C. P. Doncaster, *Timetable of human evolution and cultural development.* [Online] Available: http://www.southampton.ac.uk/~cpd/history.html. Accessed on: 19-Jul-19.

[2] R. L. Kelly, "Hunter-gatherer mobility strategies," *Journal of anthropological research*, vol. 39, no. 3, pp. 277–306, 1983.

[3] B. Bender, "Gatherer-hunter to farmer: A social perspective," *World Archaeology*, vol. 10, no. 2, pp. 204–222, 1978.

[4] P. N. Stearns, *The industrial revolution in world history*: Routledge, 2018.

[5] Y. Masuda, *The information society as post-industrial society*: World Future Society, 1980.

[6] A. Rojko, "Industry 4.0 concept: background and overview," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 11, no. 5, pp. 77–90, 2017.

[7] S. M. L. Coalition, Ed., *Implementing 21st century smart manufacturing*, 2011.

[8] L. M. Fonseca, “Industry 4.0 and the digital society: concepts, dimensions and envisioned benefits,” *Proceedings of the International Conference on Business Excellence*, vol. 12, no. 1, pp. 386–397, 2018.

[9] H. Faruqee and M. Mühleisen, "Population ageing in Japan: demographic shock and fiscal sustainability," *Japan and the World Economy*, vol. 15, no. 2, pp. 185–210, 2003.

[10] Y. Shiroishi, K. Uchiyama, and N. Suzuki, “Society 5.0: For Human Security and Well-Being,” *Computer*, vol. 51, no. 7, pp. 91–95, 2018.

[11] S. Teufel and B. Teufel, “The Positive Momentum of Crowds for the Implementation of Smart Environments,” *Proceedings International Conference on Social Sciences and Management*, Beijing, China 2019.

[12] M. N. Wexler, “Reconfiguring the sociology of the crowd: exploring crowdsourcing,” *International Journal of Sociology and Social Policy*, vol. 31, no. ½, pp. 6–20, 2011.

[13] J. Vasauskaite, S. Teufel, and B. Teufel, “Smart Framework: Application under the Conditions of Modern Economy,” *Inzinerine Ekonomika-Engineering Economics*, vol. 28, no. 2, pp. 180–186, 2017. doi: 10.5755/j01.ee.28.2.17631.

[14] D. Sangokoya, *5 challenges for civil society in the Fourth Industrial Revolution* | World Economic Forum. [Online] Available: https://www.weforum.org/agenda/2017/12/5-challenges-facing-civil-society-in-the-fourth-industrial-revolution/. Accessed on: 15-Oct-19.

[15] T. Takahashi, “Behavioral Economics of Addiction in the Age of a Super Smart Society: Society 5.0,” (en), Oukan, vol. 12, no. 2, pp. 119–122, https://www.jstage.jst.go.jp/article/trafst/12/2/12_119/_pdf, 2018.

[16] M. Aldabbas and B. Teufel, “Human Aspects of Smart Technologies’ Security: The Role of Human Failure,” *JOURNAL OF ELECTRONIC SCIENCE AND TECHNOLOGY*, vol. 14, no. 4, pp. 311–318, 2016.

[17] D. J. Brooks, “What is security: Definition through knowledge categorization,” *Security Journal*, vol. 23, no. 3, pp. 225–239, 2010.

[18] S. Marinkovic, S. Christian, and P. Emanuel, "Energy-efficient TDMA-based MAC protocol for wireless body area networks," in *Proceeding of the 3rd International Conference on Sensor Technologies and Applications*, Athens, Greece, 2009, pp. 604-609.

[19] G. Fang and E. Dutkiewicz, “Bodymac: energy efficient tdma-based mac protocol for wireless body area networks,” in *Proceeding of the 9th International Symposium on Communications and Information Technology*, Icheon, South Korea, pp. 1455–1459.

[20] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, “Position based cryptography with location privacy: A step for fog computing,” *Future Generation Computer Systems*, vol. 78, pp. 799-806, January 2018.

[21] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, “A comprehensive survey on fog computing: State-of-the-art and research challenges,” *IEEE Communication Surveys & Tutorials*, vol. 20, no. 1, pp. 416-464, 2017.

[22] J. Ni, K. Zhang, X. Lin, and X. Shen, “Securing fog computing for Internet of Things applications: Challenges and solutions,” IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 601-628, 2017.

[23] H. Silva, B. Felipe, and N. Augusto, "Cross-layer multiuser session control for improved SDN cloud communications," in *Proceeding of 2018 International Conference on Computing, Networking and Communications*, Maui, USA, 2018, pp. 377-382.

[24] M. Sohail, S. Khan, R. Ahmad, D. Singh, and J. Lloret, “Game theoretic solution for power management in IoT-based wireless sensor networks,” *Sensors*, vol. 19, no. 18, pp. 3835, 2019, DOI: 10.3390/s19183835.

[25] X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos, “Knowledge-aware proactive nodes selection approach for energy management in Internet of things,” *Future Generation Computer Systems*, vol. 92, pp. 1142-1156, March 2019.

[26] J. Ren, Hui Guo, Chugui Xu, and Yaoxue Zhang, “Serving at the Edge: A scalable IoT architecture based on transparent computing,” vol. 31, no. 5, pp. 96-105, 2017.

[27] W. X. Ding, X. Y. Jing, Z. Yan, L. T. Yang, “A survey on data fusion in Internet of things: Towards secure and privacy-preserving fusion,” *Information Fusion*, vol. 52, pp. 129-144, November 2019.

[28] W. Xu and J. Yu, "A novel approach to information fusion in multi-source datasets: A granular computing viewpoint," *Information Sciences*, vol. 378, pp. 410-423, February 2017.

[29] F. H. Bijarbooneh , W. Du , E. C. H. Ngai , X. Fu , and J. Liu, “Cloud-assisted data fusion and sensor selection for Internet of things,” *IEEE Internet Things Journal*, vol. 3, no. 3, pp. 257-268, June 2016.

[30] R. Miotto, F. Wang, S. Wang, X. Q. Jiang, and J. T. Dudley, “Deep learning for healthcare: Review, opportunities and challenges,” *Briefings in Bioinformatics*, vol. 19, pp. 1236-1246, November 2018.

[31] C. Shi, Y. T. Li, J. W. Zhang, Y. Z. Sun, and P. S. Yu, “A survey of heterogeneous information network analysis,” *IEEE Trans. on Knowledge and Data Engineering*, vol. 29, pp. 17-37, January 2017.

[32] K. Hasan, K. Biswas, K. Ahmed, N. S. Nafi, M. S. Islam, “A comprehensive review of wireless body area network,” J*ournal of Network and Computer Applications*, vol. 143, pp. 178-198, October 2019.

[33] M. Mehrnoush and S. Roy, “Coexistence of WLAN network with radar: Detection and interference mitigation,” *IEEE Trans. on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 655-667, December 2017.

[34] L. F. Mohaisen, L. L. Joiner, L. F. Mohaisen, *et al*., “Interference aware bandwidth estimation for load balancing in EMHR-energy based with mobility concerns hybrid routing protocol for VANET-WSN communication,” Ad Hoc Networks, 2017, 66:1–15.

[35] Y. Chen, M. Li, P. Chen, and S. Xia, “Survey of cross-technology communication for IoT heterogeneous devices,” *IET Communications*, vol. 13, pp. 1709-1720, July 2019.

[36] Y. Liu, Z. Qin, M. Elkashlan, *et al*., “Nonorthogonal multiple access for 5G and beyond,” *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2347-2381, December 2017.

[37] J. H. Hauer, V. Handziski, and A. Wolisz, “Experimental study of the impact of WLAN interference on IEEE 802.15.4 body area networks,” in *Proceeding of European Conference on Wireless Sensor Networks*, Berlin, Germany, pp. 17–32, 2009.

[38] K. Staniec and G. Debita, “Interference mitigation in WSN by means of directional antennas and duty cycle control,” *Wireless Communications & Mobile Computing*, vol. 12, no. 16, pp. 1482-1492, December 2010.

[39] W. Scanlon, W., Conway, G., Cotton, S., “Antennas and propagation considerations for robust wireless communications in medical body area networks,” in *Proceeding of IET Seminar on Antennas and Propagation for Body-Centric Wireless Communications*, pp. 37-42, 2007.

[40] M. Patel and J. Wang, “Applications, challenges, and perspective in emerging body area networking technologies,” IEEE Wireless Communications, vol. 17, no. 1, pp. 80-88, February 2010.

[41] A. Kiourti and K. S. Nikita, “A review of implantable patch antennas for biomedical telemetry: Challenges and solutions [wireless corner],” *IEEE Antennas and Propagation Magazine*, vol. 54, no. 3, pp. 210-228, 2012.

[42] H. Cao, V. Leung, C. Chow, and H. Chan, “Enabling technologies for wireless body area networks: A survey and outlook,” *IEEE Communications Magazine*, vol. 47, no. 12, pp. 84-93, December 2009.

[43] R. Cavallari, F. Martelli, R. Rosini, *et al*., “A survey on wireless body area networks: Technologies and design challenges,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1635-1657, February 2014.

[44] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Computer Networks*, vol. 76, no. 15, pp. 146-164, January 2015.

[45] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The Internet of things: Review and theoretical framework," *Expert Systems with Applications*, vol. 133, pp. 97-108, November 2019.

[46] I. U. Din, M. Guizani, S. Hassan, B. S. Kim, M. K. Khan, M. Atiquzzaman, and S. H. Ahmed, "The Internet of things: A review of enabled technologies and future challenges," *IEEE Access*, vol. 7, pp. 7606-7640, January 2019.

[47] S. Sicari, C. Cappiello, F. De Pellegrini, D. Miorandi, and A. Coen-Porisini, "A security-and quality-aware system architecture for Internet of things," *Information Systems Frontiers*, vol. 18, no. 4, pp. 665-677, August 2016.

[48] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of things," *Journal of Network and Computer Applications*, vol. 42, pp. 120-134, June 2014.

[49] J. H. Ziegeldorf, G. M. Oscar, and W. Klaus, "Privacy in the Internet of things: Threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728-2742, December 2014.

[50] Q. C. Zhang, L. T. Yang, Z. K. Chen, P. Li, and F. Y. Bu, "An adaptive dropout deep computation model for industrial IoT big data learning with crowdsourcing to cloud computing," *IEEE Trans. On Industrial Information*, vol. 15, no. 4, pp. 2330-2337, April 2019.

[51] S. Li, Y. Jia, X. Wu, A. Li, and X. Yang, "Techniques of big data security from the perspective of life cycle management," *Big Data Research*, vol. 3, pp. 2017047-1-17, May 2019.

[52] T. K. Dang, D. M. C. Pham, and D. D. Ho, "On verifying the authenticity of e-commercial crawling data by a semi-crosschecking method," *International Journal of Web Information Systems*, vol. 15, pp. 454-473, October 2019.

[53] Y. Li and H. Zhou, "Bagging eEP-based classifiers for junk mail classification," *International Journal of Security And Its Applications*, vol. 10, pp. 121-128, March 2016.

[54] Q. Mo and K. Yang, "Overview of web spammer detection," *Journal of Software*, vol. 25, no. 7, pp. 1505-1526, July 2014.

[55] F. Arute, K. Arya, R. BABBUSH, *et al*., "Quantum supremacy using a programmable superconducting processor," *Nature*, 2019, vol. 574, no 7779, pp. 505-510, October 2019.

[56] H. L. Tian, Y. Zhang, X. H. Xu, *et al*., "TrustedSSD: New foundation for big data security," *Chinese Journal of Computers*, vol. 39, no. 1, pp. 154-168, January 2016.

[57] D. G. Feng, M. Zhang, H. Li, "Big data security and privacy protection," *Chinese Journal of Computers*, vol. 37, no. 1, pp. 246-258, January 2014.

[58] J. G. Han, M. X. Bei, L. Q. Chen, *et al*., "Attribute-based information flow control," *Computer Journal*, vol. 62, pp. 1214-1231, August 2019.

[59] A. S. Mário, K. Chatzikokolakis, Y. Kawamoto, and C. Palamidessi, *et al*., "A game-theoretic approach to information-flow control via protocol composition," *Entropy*, vol. 20, no. 5, pp. 382: 1-43, 2018.

[60] D. Zhang, Y. F. Li, and Z. Zheng, "A secure sharing mechanism for data resources in cloud computing," *Netinfo Security*, no. 8, pp. 79-82, 2012.

[61] N. Seeman, "Data anonymity, not 'digital consent'," *Nature*, vol. 573, p. 34, September 2019.

[62] W. J. Meng, J. H. Ge, and T. Jiang, "Secure data deduplication with reliable data deletion in cloud," *International Journal of Foundations of Computer Science*, vol. 30, pp. 551-570, April 2019.

[63] L. Xue, Y. Yu, Y. N. Li, M. H. Au, X. J. Du, and B. Yang, "Efficient attribute-based encryption with attribute revocation for assured data deletion," *Information Science*, vol. 479, pp. 640-650, April 2019

[64] M. Fukuyama, "Society 5.0: Aiming for a New Human-Centered Society," *Japan SPOTLIGHT*, pp. 47–50, 2018.

[65] V. Ducrot, "Herausforderungen für die Mobilität von morgen," presentation as part of the lecture "Fribourg von morgen", iimt, University of Fribourg, 2019.

[66] P. Prisecaru, "Challenges of the fourth industrial revolution," *Knowledge Horizons. Economics*, vol. 8, no. 1, p. 57, 2016.

[67] L. Floridi, "Soft Ethics and the Governance of the Digital," Philosophy & Technology, vol. 31, no. 1, pp. 1–8, https://doi.org/10.1007/s13347-018-0303-9, 2018.

[68] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd Annual Design Automation Conference*, San Francisco, California, 2015, pp. 1–6.