# *Social ethics in Internet of Things:An outline and review*

Amin Shahraki
Faculty of Computer Sciences/ Department of Informatics
Østfold University College/ University of Oslo
Halden / Oslo, Norway
Amin.shahraki@hiof.no

Øystein Haugen
Faculty of Computer Sciences
Østfold University College
Halden, Norway
Oystein.haugen@hiof.no

*Abstract*— **Internet of Things(IoT) is still in infancy. There are concerns that IoT can jeopardize privacy as side-effects of providing the desired services. Social effects of IoT should be considered as an important part of IoT-human interaction. The interaction between IoT entities and people's lives makes it more necessary to have full transparency such that people themselves can evaluate how the IoT affects their lives. Trust between people and IoT industry is a significant issue for a more mature IoT. This paper reviews the different aspects of social ethics in IoT including equity, equality, and trustability. Effects of IoT in social human life and vital factors are explained. We review different factors that can increase the acceptance of IoT. The core of the paper is designing a guideline to interact with IoT from a social perspective. Finally, general policies are suggested for a roadmap for the future.**

***Keywords: Internet of Things, Social Ethics, Ethical Issues, IoT policies, Cyber Physical Systems.***

## I. Introduction

During the last decade, Internet of Things(IoT)[1] has been emerging as a new phenomenon that will change the world. IoT will make an impact on different aspects of human life such as the economy, welfare, security, safety, etc. There are a lot of applications for IoT like smart homes, smart cities, healthcare, etc.[2]. IoT establishes interrelated computing devices, where each one has a unique identifier and can communicate with each other with minimum human intervention. RFID[3] and sensors can make objects detectable and gather data from a monitored environment respectively. Generally, RFID tags are embedded or attached to objects that can be identified and tracked in a monitored environment[4]. In addition, there are different sensors that can help IoT to monitor the environment such as temperature or moisture sensors, cameras as multimedia sensors, motion or vibration sensors [5]. Objects like cars, home appliances or clothes can connect to the Internet for analysis of their gathered data. Also, virtual objects such as social networks are an integral part of IoT[6]. Virtual objects, like a Twitter account, can communicate with Internet services to analyze user's location, behavior or emotions without human intervention. Based on the extracted information, other agents will do reactions to control the environments physically or virtually.

IoT is changing the Internet essence. The traditional Internet is based on connecting people or machines and transferring data which are controlled by users. IoT connects entities which can be independent from humans and transfer data to make decision autonomously. Although there are a lot of ethical issues on the Internet[7], IoT creates new ethical challenges, technically and socially based on the IoT nature. These ethical issues are integrating with human life and privacy. IoT accesses to user's data, location, behavior and even mind. It can be used to misuse information and control user's lives by security attacks such as identify theft, selling information, endangering safety, etc. On the other hand, there are lots of concerns about social inequalities or loss of trust[8]. These concerns can make an impact on efficiency and acceptance of IoT and finally may change users' attitude. IoT is still in infancy, so there are ethical issues which have not been expressed and other issues which have not emerged at the moment, but they will appear in the future when IoT develops. Although technical concerns are important, this paper only focuses on social concerns and issues which can help the society to be ready for IoT.

There are several efforts to propose regulations to support IoT development. Data Protection Regulation (DPR) has been proposed by EU to support the privacy of data created by new technologies[9]. It tries to propose regulations that can protect personal data based on different processing forms. Also, White House in the USA introduces a framework to protect the privacy of network consumers based on respecting for context and individual control[10]. Consumer Bill of Rights as a main part, include controlling personal data in companies by individuals. Weber et al. in [11] survey fundamental issues to guarantee data protection in the networked world. Main challenges and rules of data protection were considered. Lunshof et al. in [12] argue that having access to any raw data should consider as a moral right. In [13] authors provide a comprehensive survey about different aspects of security and privacy in Cyber-physical systems, especially in IoT. Also, In [14], Jeschke et al. survey Industrial IoT and present future security and privacy challenges. Brey in [15], anticipate the ethical issues in emerging IT technologies such as Cyber-physical systems. In addition, Weinberg et al. in [16] argue about different aspects of IoT advantages against security

978-1-5386-6531-2/18/$31.00 ©2018 IEEE

issues. Sicari et al. in [17] explain the future of security and privacy in IoT and try to draw a roadmap for future.

In section II different social issues will be reviewed based on IoT and users' interaction. In each part, main concerns and dilemmas will be explained and alongside solutions. In Section III different policies will be expressed to design an outline for future.

## II. Social Issues

IoT raises several social issues. Already we have issues with the Internet such as fair access for all, accessing to private information, etc. These issues can migrate to IoT with different shapes. IoT is integrating with human life. It has access to more private and valuable information in comparison with the traditional Internet such as health, location, behavior or emotions. To increase the acceptance of IoT, such information should be safe and secure. Furthermore, there are concerns directly related to the IoT. Such concerns can influence people to stop using IoT believing it to be an interference or malicious technology. In this section we discuss aspects which can strengthen general negative or positive believes about IoT.

### *A. Trust*

In traditional Internet, one of the most important concerns has always been trust. An entity that can be a person, object or a service must trust other entities to start interacting with them. In a trust process, there are two entities, trustor and trustee. A trustor is an entity that trusts a trustee. One of the best definition for trust that can cover the Internet phenomenon is "Trust is the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective to the ability to monitor or control that other party"[18]. There are two issues regarding IoT and trust: 1. Trusting entities that you share information with 2. Trusting that the information is not shared with others than those you know about. When everything is connected to the Internet, it is really hard to trust that information is only shared with those declared. Most of IoT objects will communicate with each other without human intervention[19]. Interoperability is an important issue in IoT that tries to connect different objects with different technologies to each other by using middleware or cloud technology. Also, in most cases, IoT nodes use other nodes to transfer data to a destination. RPL is well-known routing method in IoT to transfer data which is based on using other nodes as routers.[20] Providing the safety of private information during transferring or connecting to other machines is a significant duty of IoT infrastructure. In addition, from business perspective view, when a new equipment is introduced as IoT object, people will assess whether it is trustable or not. If the amount of untrustable IoT equipment is high, people cannot trust the whole IoT infrastructure and will reject that IoT technology. By considering that most people are not experts in the field of IoT to assess the equipment, they will trust vendors and experts. There are some efforts to evaluate IoT devices. As an example, Shodan[21] is a search engine to evaluate the trustability of connected devices. Trust should be an integral part of the IoT development rather than an optional extension. A security problem can change users' ideas for use IoT equipment, especially when it is related to their safety. For instance, if there is a smart car that can be hacked remotely through IoT, it is really hard to convince people to buy other smart cars[22]. Researchers and industry should be careful when they are designing a new IoT equipment and not sell it when there are still security concerns. By considering that IoT is an emerging technology, this is the best time to experiment with IoT technology and realize that what policies and methods are needed to make IoT trustable and get feedback to improve them. After some years, IoT will be in full operation and it would be hard and costly to change the infrastructure. When it comes to safety, most people cannot trust equipment with even small concern. Hacking a car can kill someone, hacking an email can misuse information. They are not comparable in terms of trust for ordinary people. A technology that cannot provide safety will be rejected. As an example, Tesla autopilot system failed to detect an upcoming obstacle and caused a crash in May 2016. Although the accident had no major impact on Tesla sales, such problems may change people mind about smart cars for a long time[23]. Trust management in IoT [24] is a topic that is based on providing trust in different aspects such as data mining, services and user privacy. One of the most important sub-topics in trust management is reputation systems[25]. Reputation systems collect and analyze data about different entities. They can be used to characterize objects. By using gathered datasets, users and other entities can make decisions about trust. Reputation systems can evaluate IoT entities and the level of trustability. They can estimate agent behavior in future based on previous observations. There are some attempts to use reputation systems in IoT regarding evidences to evaluate the IoT entities' trustworthy[26, 27]. As an example, in [28] authors introduce a reputation model for MQTT protocol that can assign scores to participants based on network behavior.

### *B. Social Equity*

The term of social equity has been defined by National Academy of Public Administration as "The fair, just and equitable management of all institutions serving the public directly or by contract; the fair, just and equitable distribution of public services and implementation of public policy; and the commitment to promote fairness, justice, and equity in the formation of public policy.". The social equity is based on allocating more resources to people that need more based on their condition. People with disabilities or elderlies are examples of groups that should be given more than average. The suppliers of support tools for elderlies need to make sure their tools are particularly safe and comfortable. IoT provides the opportunity to achieve social equity at a low cost for society. Although IoT can help to support social equity, there are concerns that can prevent it. Emerging technologies may need economic incentives to be affordable by less fortunate groups such as disabled or elderly. Governments need to provide such incentives e.g. through taking an active part in the technological development and early acquisitions for early uptake of promising technology[29]. Governments should provide them without considering that it is financially profitable or not. On the other hand, IoT can help the society to provide special services cheaper and easier. Some years ago, elderlies who lived in their home, need nurses to check their condition in a regular basis. Now, IoT helps to have smart homes which check home residence all the time without human intervention and spending a lot of money. IoT can be less intrusive than people. An example is related to elderly people with incontinence where IoT sensors are put in their diapers such that it is not necessary to perform controls all the time. This both saves time and preserves dignity.

It is estimated that in 2025 the impact of the IoT will be between $2.7 trillion to $6.2 trillion on the world economy[30]. Fig. 1 illustrate the projected market share of IoT applications by 2025[30]. By supporting minorities that need more services from the government and researchers, providers will invest in designing special equipment and services for them. In some cases, vendors can provide different services permanently based on people's condition. Internet cost can be based on people's income or based on their applications. When people want to access YouTube to learn, they might pay less than they want to watch a movie regarding their data usage.

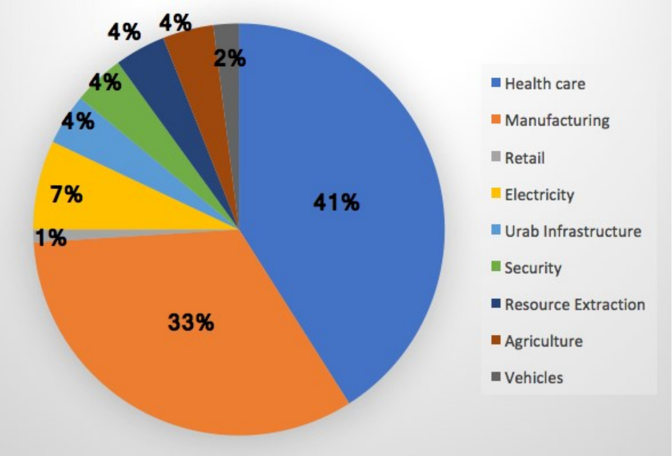

Fig. 1. Potential Economic Impact of IoT applications

Real-time applications are concrete examples of social equity in IoT[31]. Without paying attention to users, real-time applications should be supported by IoT infrastructure having higher priority temporarily. The IoT infrastructure should be designed based on allocating resources to real-time applications, especially when it is related to the safety. As an example, there is a smart car on autopilot system. There will be a car crash in a second unless the car avoids the accident. A critical safety issue is more important than another car service that wants to download music. It does not matter that the infrastructure should stop downloading music to provide safety for other people.

Digital divide is another aspect of Social Equity. Different people have different capabilities to use and interact with IoT. In addition, different groups of people are vulnerable to the technology such as children surfing the web or using a device which is able to publish contents such as smart TVs. Providing a content based IoT platform can help to recognize different groups of people and appropriate contents to support equity. Weber in [32] mentions that all IoT customers have the right access to equitable and non-discriminatory IoT infrastructure.

### *C. Social Equality*

IoT has an infrastructure that governments and service providers are designing and implementing. One of the most important things in IoT is quality of service(QoS) and fair access to the bandwidth[33]. There are different technologies that will connect objects to the Internet and provide QoS. 5G is a good example of technology that may become important for the future IoT[34]. It should support social equality by providing a minimum QoS for all users. In 2019, about 65% of the whole Internet traffic in the world is based on Mobile Networks[35]. The first and obvious issue is that 5G should be a basic service provided to all citizens for free like radio broadcasts and roads. An appropriate connection that can support typical applications, especially safety, is a basic right. In some cases, IoT needs a minimum quality to support applications. As an example, for nursing homes and support healthcare applications, there is a big need to have the high and fast bandwidth to detect heart attacks as soon as possible. The minimum QoS should support all critical services with the best quality. It is obvious that to have a better service, people should pay more. Now, the Internet is based on "best effort" services[36]. Although there is a lot of research on guaranteed service on the Internet, we have not such a service in real-world applications[37]. So, the infrastructure should be designed to provide a minimum QoS which completely support critical services such as safety services. In addition, it would be of use for the authorities and be reliable to reach the whole population in emergencies. There should be rules to supply minimum resources for all people in a network to access the Internet which can provide safety and essential applications. In other words, essential services must be kept separate from non-vital services such as entertainment and welfare services. The essential services must be provided to all free of charge as socialism. Essential services should have guaranteed QoS and be equal for all people. Bandwidth as an important factor, should reliable during a connection to support social equality.

### *D. Privacy and Transparency*

There are services in IoT that can jeopardize the privacy and help the service users at the same time. Smart TVs which are controlled by your gesture can make your life easier and can analyze your life as well[38]. There is a fine line between misusing information and helping people. If people want to take advantage of IoT, it is unavoidable that in most of the cases IoT objects can gather user's data and analyze them. Cellphones can track users if they want to use GPS. From the business perspective, having an evidence of misusing should be an alarm for providers. After having more cases, people will not trust the IoT technology and it is really hard to convince them that the equipment has no privacy problems.

Now, there are a lot of concerns that the technology is jeopardizing the privacy [39, 40]. It is normal that people have some doubts and concerns when they want to use a new emerging technology, especially when the technology can access their private information. People need to know that their information will not be misused or stored when there is no need. There should be strict rules against providers that want to gather data which are not related to their services. But there are some related issues to solve the problem as it is not so easy as we think. As an example, the data is moved across borders. Cloud systems know no borders. The data are used in places where the laws are not adequate, or they do not care much about anybody who are not their citizens. There are rumors about vendors that make a profit by selling private information. It is provider's duty to convince people that their services are safe and secure. People should know about the rules and their rights. They should control their information and accesses and be autonomous to give permission to IoT entities to access their information. They need rules that are enforced by the authorities (by law) to control the collection and use of data. To a certain extent, we already have such laws, but one should consider how IoT changes the game[41]. Service users should be able to track their information and check that the providers are not misusing or sharing their information to make a profit[42]. It can be done by other trustable providers and services that support people's privacy like Shodan[21]. Also, providers should know that someone is checking them all the time. Privacy is a highly significant issue that should be supported by everyone, government, people and providers. One of the most important solutions that can help privacy is do not storing user's data. People should be confident that their information will not be stored and analyzed at a later point in time. When there are services that need to store data to help people, an expiration date can help to remove data after a while. Also, we need to check that after expiration date, data has been removed. The impossibility of using the information as evidence in courts or legal procedures can remove some incentive factors to store data by a government as well. Also, unexpected advertisements which are based on user's private information should be prosecuted and punishable.

There are some exceptions to these topics. In some cases, users have no right to control the data. As an example, although health information is private, failing to inform a partner that he/she has AIDS is subject to punishment. IoT is able to control private information autonomously. As an example, when a smart car detect that the driver has too much alcohol in the blood, it should not start the engine. But it seems that the current technology level is unable to make complete decisions autonomously. Regarding respect to the privacy, the level of making decisions by IoT devices should be controlled and deduct to a very certain level.

### E. *Ethical algorithms*

When it comes to safety and security, IoT should provide equal and concrete services for all people. Researchers try to design algorithms and protocols that can provide the maximum safety and security for people, but when an algorithm is for more than one person as a user, who can decide which user should be given priority? When we have a world of autonomous cars, what decides the actions that determine who will die in an upcoming crash? Designing algorithms that can consider ethical issues as a factor is a novel aspect of IoT[43]. There are different ways to address the problem. One way is based on the chance of success. When there is more chance for a person to survive, IoT should focus on that person. Regarding this aspect, there is a new concern that IoT will leave another person(s) without any help, just by considering that they have less chance to survive. It seems that it is not fair and opposite of social equality. Having a trade-off can help the system to make a better decision based on users' conditions. In most cases, the time complexity of such algorithms is high and there is not enough time to process the situation completely[44]. Based on processing power, most of IoT objects are not able to process a huge amount of data. Also, they need information about other objects, so gathering data takes time[45]. Having very high bandwidth and Cloud services can help to reduce time, although there is still delay that is harmful in critical-real time situations. On the other hand, an object can use greedy models to the survival of itself. This model can help its owner to survive but can hurt others as well. So, objects should follow rules that they cannot hurt other people or minimize and balance injuries. Although this idea can help algorithms to be more ethical, it is greedy. Also, time complexity is still a problem. In addition, if a smart car has to injure others to help the driver survive, can anyone blame it? In most cases, people make greedy and selfish decisions to survive themselves and their families. So, there is a need to design models that can minimize damages. It seems that trade-off models can be a good solution for ethical algorithms to minimize damages, although the time complexity and delay should be considered as the most important metrics to evaluate them. Also, the other moral dilemma is about power over decisions. we foresee that we will leave more and more to the IoT infrastructure which is contrary to a moral of maximum freedom for the individual. Who controls the algorithms of the infrastructure? What about dissenters i.e. cars and people that do not behave according to protocol?

### F. *Autonomy*

There are two aspects of being smart in IoT. First, a node can manage itself without human intervention. It can connect to the network, transfer data, find any problem and solutions to be connected and so on. Self-configure[46] and self-healing[47] IoT networks are two aspects of being autonomous. The other aspect is about being autonomous in making decisions. A smart car can access the calendar and make an appointment with a car service company when a time of service is near. It can find a suitable time based on user's life style and calendar without getting confirmation from the user. In such a situation, the car is completely autonomous and can jeopardize the privacy. Designing a technology that can work without human intervention is great, but most people do not want a completely autonomous car[48]. Obviously, cars should interfere to control car and drive safe, but if they want to make a decision about users' lifestyle, users will not accept them. Objects do not know all things about users. Also, at least now, IoT services have no idea about human emotions as a significant factor to make decisions. It seems that, at least in near future, IoT services are not able to make autonomous decisions. Some people are interested in giving a grant to IoT, but It would be better if services need to get confirmations from users. There are different technologies to interact with users without disturbing them such as speech recognition systems[49]. In addition, if there is a service that wants to make a decision for users, it should not be compulsory. Unnecessary services that a car can give people should be clear and people can override the services all the time. Service that will jeopardize privacy must be explicitly turned on by its user. Being smart or supporting other services cannot be good reasons to be completely autonomous. There are some exceptions to these rules. If a user wants to use something to harm others, autonomous objects can make decisions to avoid it. As an example, the smart car can limit speed if the driver wants to drive more than legal speed.

### *G. Responsibility*

One of the most important issues between people is responsibility for actions. There is the same problem with objects. When a problem occurred, who is responsible to solve or recompense. There are two aspects of the responsibility. First, as smart and autonomous objects, they should support unexpected problems and solve them called self-healing[47]. Users can demand that a smart home has methods to encounter with fire or fake fire alarms. Zero human intervention is still a challenge [50] for IoT infrastructures that creates high responsibility for objects to solve expected and unexpected problems. To design systems that can support responsibility, we need to estimate different situations or use artificial intelligence methods such as machine learning to find solutions. There are a lot of efforts to design such systems that can support themselves without human intervention and response for different problems[51].

The second aspect is about the responsibility according to law. When a problem occurred by using an IoT object, who is responsible?[52] What may become a problem is that there will be objects where it is unclear who the responsible juridical person behind it is. At the moment, there is no clear answer to that question. Technology development is so rapid in compare to policies and regulations. Although providers consider as the first options to be responsible, government and individuals are also responsible in terms of issuing certificates and incorrect usage respectively. American National Institute of Standards and Technology (NIST) is working on IoT standards. Designing framework that can assign responsibility and determine the contribution of individuals and corporations is a goal in social ethics, however, IoT is still in infancy and no one can create comprehensive laws about a technology that is not completely clear. There is a strong need to change laws and regulations with technology development simultaneously.

### *H. Hidden services*

IoT can connect to users' whole life. Typically, hidden services are related to a collection of data that users are not aware of, or that can be used for other purposes by the collector. Users should know what are the services they are receiving and what information they are sharing. The hidden services that analyze user behaviors without informing the subjects should not be permitted. If there is a motion sensor in a home, it should not profile residents' behavior to conserve more energy without informing them. People will reject technologies that want to cheat them. Although a company does not want to misuse information, it is not admissible to have hidden services in their equipment. When objects do not want to transfer and store user's data, it seems that hidden services have no problem. It is an exception that although people do not know about the service, it cannot jeopardize the privacy. However, it can make general distrust in society.

### *I. Determining Personal Data*

One of the most important issues in IoT is Big Data. It refers to the concept of voluminous datasets which are complex and probably contain unstructured data such as video, audio, etc. The volume of the huge amount of data makes them difficult to control and analyze. Also, analyzing unstructured data is not easy as structured data and consume a lot of resources. From the social ethics perspective, determining personal data and separating them from other data is the main issue to protect privacy. Although there is need to protect all data, protecting personal data has higher priority regarding jeopardizing privacy. On the other hand, one of the main advantages of IoT is providing data which can be monetized. Preventing and hardening access to all data sets can turn this advantage into a disadvantage. There are some methods that can help to recognize personal data. Privacy Enhancing Measures and Privacy Enhancing Technologies are useful in this field[53], however, they have been faced with a lot of economic problems to implement in real markets[54]

Another issue is connecting a data to a person. IoT data are gathered from physical world which basically includes data related to individuals. A data set can contain data where it is hard to determine the level of correlation between each piece of data and an individual person. As an easy example, a Video can contain individual faces and traffic jams. Determining personal data and the level of relationship to a person is a hard task to implement. Nissenbuam et el. in [55] mention that "context" is a very significant factor related to the privacy protection. Locations, culture, religion, agreements, etc. can shape the contexts which can help to design frameworks for IoT. It seems that after collecting data, recognizing process would be harder based on the amount of data, so fog and edge computing can help to recognize them close to the source.[56]

## III. General policies

Researchers and providers are working on different aspects of IoT to establish a concrete infrastructure. There is a strong need to follow some policies that support social issues.

They make IoT more comfortable, trustable and accessible for people. Since IoT is emerging, it is the best time to establish rules for IoT infrastructure. Changing the IoT infrastructure will be costly and probably impossible after a while.

### A. *Being optional*

In future, IoT will connect to most of the people's life. Governments will force people to buy smart cars to reduce accident statistics and air pollution. Housebuilders should follow rules for energy conservation and use IoT equipment in homes. Although the IoT will be an important part of peoples' life, there should be options to live without non-mandatory technologies. IoT will make people's life easier, but the technologies should not force people to work with them, at least when there is no necessity. IoT should benefit people, not disturb them or make a decision for them autonomously. As an example, some insurance companies ask customers to attach an IoT gadget to their cars to monitor driving behavior. Based on driving behavior, they will reduce and increase the cost of insurance[57]. Now, it is not obligatory and people can drive traditionally. After some years, smart cars will be commonplace. Based on reducing accident statistics and air pollution, the IoT gadget will not be optional and insurance companies or government force people to use it all the time. On the other hand, if users do not want to use welfare systems in their homes, it would be optional and no one can force them to use welfare systems.

### B. *Notices*

When it comes to advertisements, companies want to describe their product as safe and secure. It should be mandatory to declare weakness and consequences for users. As an example, users should know that there is a possibility that autopilot system in their car is not able to work in traffic jams as well as highways.

### C. *Human Preferences*

One of the concrete rules that can help IoT to be more safe and secure is human preferences. The safety of a human is much more important than everything. Algorithms must be as ethical as a human being. We can demand that things should be sacrificed before humans. There should not be justification that can exchange the role of humans and objects in terms of safety. Cost or scarcity might not make an impact on human safety. In other words, smart objects should follow rules to provide safety for people without considering that they should sacrifice themselves or other objects.

### D. *Force*

Government, providers or individuals can force people to share their information. An employer who is considering users for jobs can persuade them to share private health information which is not related to the job. Rules to show what types and levels of information each company can access are useful. Also, any coercion should be prosecuted. As an example, it would be illegal, if a company asks an employee to attach a RFID tag to track all the time, even in home based on their security rules.

### E. *Comprehensive regulations and rules*

Comprehensive regulations and rules should be available for individuals and corporations to follow. Without having regulations, there is no possibility to enforce providers and individuals to obey. Also, after occurring a problem, they will not be responsible, if there is no rule to show their responsibilities. Corporations such as NIST or World Governance Index (WGI) are working to provide better regulations and rules, however by considering that IoT will be used in different countries, there is a need to provide agreements that are supported by different countries and providers. Having concrete regulations and agreements can help to solve international issues in terms of using IoT. It is obvious that agreements should be issued when IoT technology is emerging simultaneously.

## IV. Conclusion

In this paper, different aspects of social ethics in IoT are reviewed. We have also designed an outline to express map road for future. Based on different concerns, there is no possibility to delegate all actions to IoT objects and be completely safe and secure. There is a strong need to check them in a regular basis and accept their decisions. Providers of IoT infrastructure should be checked on a regular basis to avoid misuse. By considering that IoT is still in infancy, consequences of misusing user's information can make an impact on IoT future and trustability. Laws and regulations that support user's rights must be mandatory. It must be made clear that voluntary permissions cannot overrule public interests as defined by the laws. Designing IoT equipment and algorithms should consider ethics as an important factor in development. Having general policies that can guide different entities to provide safe and trustable infrastructure for IoT is necessary.

## V. References

[1] K. Ashton, "That 'internet of things' thing," *RFiD Journal,* vol. 22, pp. 97-114, 2009.

[2] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Computer Communications,* vol. 54, pp. 1-31, 2014.

[3] R. Want, "An introduction to RFID technology," *IEEE pervasive computing,* vol. 5, pp. 25-33, 2006.

[4] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, 2012, pp. 1282-1285.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems,* vol. 29, pp. 1645-1660, 2013.

[6] M. Nitti, V. Pilloni, G. Colistra, and L. Atzori, "The virtual object as a major element of the internet of

things: a survey," *IEEE Communications Surveys & Tutorials,* vol. 18, pp. 1228-1240, 2016.

[7] G. Eysenbach and J. E. Till, "Ethical issues in qualitative research on internet communities," *Bmj,* vol. 323, pp. 1103-1105, 2001.

[8] B. Guo, D. Zhang, Z. Wang, Z. Yu, and X. Zhou, "Opportunistic IoT: exploring the harmonious interaction between human and the internet of things," *Journal of Network and Computer Applications,* vol. 36, pp. 1531-1539, 2013.

[9] E. E. Commission, "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data (General Data Protection Regulation)," *COM (2012) 11 final, 2012/0011 (COD), Brussels, 25 January 2012,* 2012.

[10] W. House, "Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy," *White House, Washington, DC,* pp. 1-62, 2012.

[11] R. H. Weber, "The digital future–A challenge for privacy?," *Computer Law & Security Review,* vol. 31, pp. 234-242, 2015.

[12] J. E. Lunshof, G. M. Church, and B. Prainsack, "Raw personal data: providing access," *Science,* vol. 343, pp. 373-374, 2014.

[13] H. Song, G. A. Fink, and S. Jeschke, *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*: John Wiley & Sons, 2017.

[14] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir, and T. Eschert, "Industrial Internet of Things and Cyber Manufacturing Systems," in *Industrial Internet of Things*, ed: Springer, 2017, pp. 3-19.

[15] P. A. Brey, "Anticipating ethical issues in emerging IT," *Ethics and Information Technology,* vol. 14, pp. 305-317, 2012.

[16] B. D. Weinberg, G. R. Milne, Y. G. Andonova, and F. M. Hajjat, "Internet of Things: Convenience vs. privacy and secrecy," *Business Horizons,* vol. 58, pp. 615-624, 2015.

[17] 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, pp. 146-164, 2015.

[18] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of management review,* vol. 20, pp. 709-734, 1995.

[19] L. Atzori, A. Iera, and G. Morabito, "From" smart objects" to" social objects": The next evolutionary step of the internet of things," *IEEE Communications Magazine,* vol. 52, pp. 97-105, 2014.

[20] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wireless Communications,* vol. 20, pp. 91-98, 2013.

[21] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices," *International Journal of Critical Infrastructure Protection,* vol. 7, pp. 114-123, 2014.

[22] R. Ramquist, "Proposals For The Secure Use Of IoT Technology In The Car Industry-Proposals on how to use IoT technology in the car industry but avoid its negative security consequences," ed, 2016.

[23] P. Lin. (2016). *Tesla Autopilot Crash: Why We Should Worry About a Single Death*. Available: http://spectrum.ieee.org/cars-that-think/transportation/self-driving/tesla-autopilot-crash-why-we-should-worry-about-a-single-death

[24] G. Lize, W. Jingpei, and S. Bin, "Trust management mechanism for Internet of Things," *China Communications,* vol. 11, pp. 148-156, 2014.

[25] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: A survey and taxonomy," *Journal of Parallel and Distributed Computing,* vol. 75, pp. 184-197, 2015.

[26] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Computer Science and Information Systems,* vol. 8, pp. 1207-1228, 2011.

[27] 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, 2014.

[28] B. Aziz, P. Fremantle, R. Wei, and A. Arenas, "A utility-based reputation model for the internet of things," in *IFIP international information security and privacy conference*, 2016, pp. 261-275.

[29] B. Sadowski, O. Nomaler, and J. Whalley, "Technological Diversification of ICT companies into the Internet of things (IoT): A Patent-based Analysis," 2016.

[30] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy* vol. 180: McKinsey Global Institute San Francisco, CA, 2013.

[31] S. Haller and C. Magerkurth, "The real-time enterprise: Iot-enabled business processes," in *IETF IAB Workshop on Interconnecting Smart Objects with the Internet*, 2011.

[32] R. H. Weber, "Internet of things–governance quo vadis?," *Computer Law & Security Review,* vol. 29, pp. 341-347, 2013.

[33] H. Shi, R. V. Prasad, E. Onur, and I. Niemegeers, "Fairness in wireless networks: Issues, measures and challenges," *IEEE Communications Surveys & Tutorials,* vol. 16, pp. 5-24, 2014.

[34] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel*, et al.*, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications,* vol. 34, pp. 510-527, 2016.

[35] V. K. Shukla and D. Ojha, "Proposed Concept for Ontology Communication between IOT Devices."

[36] X. Xiao and L. M. Ni, "Internet QoS: A big picture," *IEEE network,* vol. 13, pp. 8-18, 1999.

[37] S. Gorlatch, T. Humernbrum, and F. Glinka, "Improving QoS in real-time internet applications: from best-effort to Software-Defined Networks," in *Computing, Networking and Communications (ICNC), 2014 International Conference on*, 2014, pp. 189-193.

[38] B. Michéle and A. Karpow, "Demo: using malicious media files to compromise the security and privacy of smart TVs," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, 2014, pp. 1-2.

[39] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in *The Internet of Things*, ed: Springer, 2010, pp. 389-395.

[40] H. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life*: Stanford University Press, 2009.

[41] E. Z. Tragos, J. B. Bernabe, R. C. Staudemeyer, J. Luis, H. Ramos, A. Fragkiadakis*, et al.*, "Trusted IoT in the complex landscape of governance, security, privacy, availability and safety," *Digitising the Industry–Internet of Things Connecting the Physical, Digital and Virtual Worlds. River Publishers Series in Communications,* pp. 210-239, 2016.

[42] D. Klopper, "The possibilities and challenges of the application and integration of the Internet of Things for future marketing practice," University of Twente, 2016.

[43] G. Baldini, M. Botterman, R. Neisse, and M. Tallacchini, "Ethical design in the internet of things," *Science and engineering ethics,* pp. 1-21, 2016.

[44] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of things and big data analytics for smart and connected communities," *IEEE Access,* vol. 4, pp. 766-773, 2016.

[45] Y. Sun, X. Qiao, B. Cheng, and J. Chen, "A low-delay, lightweight publish/subscribe architecture for delay-sensitive IoT services," in *Web Services (ICWS), 2013 IEEE 20th International Conference on*, 2013, pp. 179-186.

[46] I. Chatzigiannakis, H. Hasemann, M. Karnstedt, O. Kleine, A. Kroller, M. Leggieri*, et al.*, "True self-configuration for the IoT," in *Internet of Things (IOT), 2012 3rd International Conference on the*, 2012, pp. 9-15.

[47] J. Ramiro and K. Hamied, *Self-organizing networks (SON): self-planning, self-optimization and self-healing for GSM, UMTS and LTE*: John Wiley & Sons, 2011.

[48] K. Kernaghan, "The rights and wrongs of robotics: Ethics and robots in public organizations," *Canadian Public Administration,* vol. 57, pp. 485-506, 2014.

[49] K. M. Lee, W. Peng, S. A. Jin, and C. Yan, "Can robots manifest personality?: An empirical test of personality recognition, social responses, and social presence in human–robot interaction," *Journal of communication,* vol. 56, pp. 754-772, 2006.

[50] D. Wang, S. Lee, Y. Zhu, and Y. Li, "A zero human-intervention provisioning for industrial IoT devices," in *Industrial Technology (ICIT), 2017 IEEE International Conference on*, 2017, pp. 1271-1276.

[51] D. Kyriazis and T. Varvarigou, "Smart, autonomous and reliable Internet of Things," *Procedia Computer Science,* vol. 21, pp. 442-448, 2013.

[52] D. Liren, "Development of IOT and Good Governance in Public Management [J]," *Public Administration & Law,* vol. 1, p. 006, 2011.

[53] J. Cave, G. Bodea, K. Kool, and M. v. Lieshout, "Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy," 2011.

[54] A. Acquisti, "Privacy and security of personal information," *Economics of Information Security,* pp. 179-186, 2004.

[55] H. Nissenbaum, "Respecting context to protect privacy: Why meaning matters," *Science and engineering ethics,* pp. 1-22, 2015.

[56] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," in *Proceedings of the 2015 Workshop on Mobile Big Data*, 2015, pp. 37-42.

[57] J. Manral, "IoT enabled Insurance Ecosystem-Possibilities Challenges and Risks," *arXiv preprint arXiv:1510.03146,* 2015.