An Exploration on Artificial Intelligence Application: From Security, Privacy and Ethic Perspective

Xiuquan Li
Institute of Science and Technology Foresight and Evaluation
Chinese Academy of Science and Technology for Development
Beijing, China
e-mail: lixiuquan@tsinghua.org.cn

Tao Zhang
College of Information Science and Engineering
Ocean University of China
Qingdao, China
e-mail: oucseczt@126.com

***Abstract*—Artificial intelligence is believed as a disruptive technology, which will change our economy and society significantly in the near future. It can be employed to replace human labors in completing many dangerous and tedious tasks, providing us with more convenient and efficient life. We can benefit a lot from the wide application of this emerging technology. However, there are also potential risks and threats in application of artificial intelligence, which need to be handled in a proper way before extensive usage. In the paper, we make discussions on the security, privacy and ethnic issues in artificial intelligence applications and point out the potential risks and threats. Countermeasures in research, regulation and supervision are suggested and our expectation for artificial intelligence development is given out.**

Keywords-artificial intelligence; security; privacy; ethics

I. INTRODUCTION

There has been 60 years development of artificial intelligence (AI) technology after the conference held at Dartmouth College in 1956, at which the term of artificial intelligence was first proposed [1]. Over the past 20 years, remarkable progress has been achieved in this area. In 2011, Watson, a cognitive system designed by IBM, beat the Jeopardy's reigning champions Brad Rutter and Ken Jennings, it's the first time that computers or non-human intelligence won human beings in quiz show. In 2016, as one of Google's artificial intelligence systems, AlphaGo achieved a big success in a match challenge with Lee Se-dol, one of the world's top go chess players.

With further maturation of AI techniques, there will likely be more robots or intelligent programs that can help us as human's assistants and do a lot for us, such as reading email, cleaning room, or even driving cars for us. However, every coin has its two sides, so does artificial intelligence. It will also bring us impact on privacy, security and ethic. Many uncontrolled consequences might arise from AI applications if we fail to identify and prevent related threats beforehand. In this study, we discuss the potential risks and threats of artificial intelligence, raise warnings and give our suggestions.

The paper is organized as follows: in section two, we introduce the concept of artificial intelligence, related techniques and their applications. In section three, we discuss the security, privacy and ethic problems in artificial intelligence application. We give out countermeasures for these issues in section four. Finally, we draw conclusions in section five.

II. ARTIFICIAL INTELLIGENCE AND APPLICATIONS

Artificial intelligence is the technology that imitates human intelligence processes by machines, especially computer systems. These intelligent processes include perception, learning and reasoning. Artificial intelligence has been introduced to relieve human labors from dangerous tasks and situation. Currently, it is being broadly used in different fields [2].

Artificial intelligence can be classified into weak AI and strong AI. In the category of strong AI, AI system is considered to have human-like high level cognition ability, such as common sense, self-awareness and creativity, while weak AI simulates human intelligent processes passively without real understanding. From task resolving ability perspective, weak AI is designed to finish a particular task, while strong AI is usually believed a general AI system, which has the ability to fulfill multiple kinds of intelligent tasks.

Current AI systems are all at the stage of weak AI and strong AI does not yet exist so far. It is supposed that it would take decades for human to realize strong AI [3]. Typical artificial intelligence techniques include machine learning, speech Recognition, natural language processing, machine vision, robot, etc.. At the moment, artificial intelligence has been used everywhere in our life, from speech text input and personalized network shopping, to various intelligent answering systems. We have benefited and will benefit in long term from AI applications in these fields such as science, engineering, education, business, medical care and manufacturing etc. [4].

1) AI application in healthcare. With the help of AI techniques, your smart home system can monitor your daily life, including your sleep time, exercise, diet preferences, and capture signs of their changes. Future toilet perhaps can detect through your excreta to determine if your body is healthy, and provide relevant information to your doctor. IBM Watson is a good example of cognitive technology

978-1-5090-4499-3/17/$31.00 ©2017 IEEE

application in healthcare. It can help professionals make medical diagnoses, increasing patient compliance and minimizing the impact of iatrogenic disease and medical errors. Such system can assist doctors in making decision without consulting specialists which are scarce resources in rural areas and in many developing countries [5].

2) AI application in finance. Industry and government can use artificial intelligence to realize early detection of abnormal financial risks and to reduce malicious behaviors such as manipulating markets, fraud and unusual transactions. There are many AI techniques, like artificial neural network and support vector machine, used by commercial bankers and business consultants to make bankruptcy prediction and company financial distress prediction [6]. AI techniques are also frequently employed to develop intelligent financial products, facilitating people's investment by providing high quality financial assistant service. Financial automation transaction is another AI based financial technology, which has shown its advantages in improving efficiency and reducing transaction cost.

3) AI application in education. AI can grade and assess students in an intelligent way and help them learn at their own pace. Based on AI technique, we can build a new education system that includes intelligent evaluation and interactive learning. With the help of intelligent education assistant, teacher can be provided with additional support by knowing the status and learning progress of each student at any time. In addition, AI techniques could be used to provide education push services for on-the-job people, changing significantly where and how people learn, or even replacing some teachers [7].

III. Security, Privacy and Ethics Threats in Artificial Intelligence Applications

As discussed above, artificial intelligence have been applied in different areas, and millions of people would benefit from that. However, Artificial intelligence may also be used to steal our private information and launch large scale network attacks by attackers. There are potential risks and threats in application of artificial intelligence. What's worse, it may cause ethical problems. It is important to make it clear the potential threats in different areas of artificial intelligence applications before they are put forward.

A. Security Problems

There are different types of security problems of AI including security threats of technology abuse, security problem induced by technical defects and self-aware intelligence evoked security problems.

1) Security threats of technology abuse. It is believed that artificial intelligence is a neutral technique. What it will bring us depends much on how to use and manage it. If it is abused by malicious people, the technique may bring us problems of security, privacy and ethic. Experiment shows that attackers can launch a large-scale attack with only a little resource when using intelligent methods [8]. Attackers may also use AI technology to access private information illegally.

If unmanned vehicles, robots and other artificial intelligence products are controlled through a illegal way, these AI systems may do something harmful to people in control of criminals. One day in the future, we may be attacked just because our artificial intelligence assistants are attacked or hijacked if this issue is not considered seriously.

2) Security problems induced by technical defects. As a developing technology, current artificial intelligence system is far from perfect. Sometimes AI system may be not as secure as it seems due to some technical defects. Thus there are security threats in AI systems. It was reported in 2005 that a worker was killed when setting up an industrial robots in Germany and a similar killing event happened in India in August. There was also a robot accident that happened in an auto parts factory in Michigan State of America in June 2015, where a failed robot on assembly line attacked a worker and led to death. In that security event, 5 companies were accused to be responsible for the accident.

There are some reasons that account for this kind of security problem. One of them is technical imperfection as robots, tools, controllers and related components are not properly designed, manufactured or tested. Another reason is improper management, causing many robotic accidents occur under unconventional operating conditions such as programming, maintenance, testing, installation or adjustment. In many of these operations, when workers stay in a robot working environment, they may encounter unexpected damage.

3) Security problems evoked by possible self-aware intelligence. The worst AI security concern is mainly about the possible that artificial intelligence develops into strong AI stage, when robots or other artificial intelligence products can self-evolve and may develop self-awareness, thus bringing about serious threat to human existence. Although strong AI is still far from realization, security issues should be considered beforehand [9].

With development of modern brain science, the study of unsupervised learning theory is making fast progress, and cognitive intelligence may make a real breakthrough one day in the near future. Some research teams in the world are studying high level cognition intelligence like machine emotion and machine awareness. Also, some scientists are exploring machine creation force and machine evolution. It is not known whether and when a strong AI will come, but the possibility still exists. It would be a security threat if super intelligence with self-aware ability could not be fully controlled by human beings.

B. Privacy Problems

In recent years, big data driven paradigm has dominated artificial intelligence research and has led to a new bloom of AI development. In current machine learning, the number and quality of data sets will affect in high degree the training results, so most of successful AI applications rely heavily on big data. As privacy problem is a main threat of data exploration, inevitably, there will also be privacy problems in the applications of artificial intelligence.

1) Privacy in data acquirement. Because of wide use of smart home devices, variety of information about you and your family can be kept for years or even decades. These data, if used properly, will make your family life better. But

some of your private information would also be used illegally by technology companies for commercial purposes.

Other data produced by electrical activities, such as pharmacy notes, mobile phone geographical coordinates and travel routes, also involve personal sensitive information. Some of these privacy information is collected by different companies for intelligent applications, which may cause privacy invasion.

2) Privacy in cloud computing. With the introduction of cloud computing, many companies and government organizations are migrating their data to cloud, because it is cheap, easy to use, and convenient in getting on-demand network access to a shared pool. When our private information is stored at cloud, our privacy need to be ensured.

Amid higher computation requirement of artificial intelligence, cloud computing has been configured as main infrastructure of many AI applications, so privacy problems are what we need to reconsider when using such intelligence techniques.

3) Privacy in knowledge extracting. As knowledge extracting tools are becoming increasingly powerful, numerous seemingly unrelated data fragments may be integrated to identify individual behavioral characteristics, thereby exposing personal privacy.

For example, when internet sites visit traces, shopping processes and other different types of record data are combined together, you can outline a person's behavior map, and may analyze their personal preferences and behavioral habits, thus further predicting the potential needs of consumers. In this way, business shops are able to provide in advance them with the necessary information, possible products or services. Personalized customization has become a major feature and highlight of current intelligent applications. But these personalized customization processes are accompanied by discovery and exposure of personal privacy, and how to avoid privacy invasion is a problem worthy of investigation.

C. Ethical Problems

As to the most special problem that rapidly changing AI technology may bring to us, almost all scientific and technological personnel will believe ethic is the focus of attention, due to the human like intelligence ability of this powerful technology. Ethical problems might be induced by following issues.

1) Behavior rule. Artificial intelligence robots must learn rules before making decisions. For example, if unmanned vehicle comes in the face of pedestrians and can't brake in time, artificial intelligence should choose whether crashing into the five people on road or turning to one pedestrian on sidewalk. If the design of intelligent agent is not integrated with the human constraints, it is likely to follow a different logic with human behavior and lead to terrible consequences. We must make these new systems benefit the whole community, not just the controller of the system, through constraining behaviors of AI systems to comply with predefined social ethic rules.

2) Role of robots. Another ethical problem we need to consider is that what the robots or machines actually are. Some ethicists claim that artificial intelligent robots have their own rights as we human beings, because robots might have emotion, sentience, cognition and intelligence in the future. So if robots have self-improving intelligence and sentience, what's the role of robots in our life?

In some key areas such as criminal justice systems and health care, many researchers have begun to explore the decision-making capabilities of AI on parole and diagnoses. But after giving decision-making power to the machine, we would be faced with not only the risk of out-of-control of AI, but also ethical problem itself, i.e. Does the robot have the qualification to do that?

3) Destroy of robots. There is a thought-provoking question about the ethic of AI system: can we kill an intelligent robot if we realize that robots are dangerous to us? The first problem in this issue is that if we can kill robots as we want. The killing of robots in the past may be an accident. However, it may be intended someday in the future. If these robots are not friendly or don't obey human beings, we must switch off them or kill them. The more serious problem in this issue is that if artificial intelligent robots have intelligence and sentience, how can we kill them successfully against their intelligent self protection behaviors and actions? All these problems should be considered beforehand in design process of such AI systems.

IV. COUNTERMEASURES AND DISCUSSIONS

Artificial intelligence is able to make human being more powerful, yet with security, privacy, ethic and other risks at the same time. We must pay attention to the problems arising therefrom and handle the threats in advance. Therefore, in the design, test, and use of robots and artificial intelligence products, a series of countermeasures are needed to ensure that AI systems could operate in control and in harmony with human.

A. Emphasizing Safety, Privacy and Ethic Research

Due to potential capabilities and complexity of AI, and its close interactions with human users, research on the safety of artificial intelligence technology is particularly important. Scholars and researchers need to emphasize more on security protection and try their best to make artificial intelligence more secure when applying artificial intelligence in more areas and fields.

1) Embedding ethic rule in AI design. When the artificial intelligence systems take actions by their own, we hope that their behavior will be able to comply with formal and informal rules that we humans need to follow, including ethical, legal rules. These rules should be considered and embedded in the AI system during development stage.

2) Making AI system more transparent and explainable. Current AI technology, especially deep learning, still works in a paradigm of black box. For such algorithms, few mechanisms is available to explain the results of them. So sometimes it's not easy to explore the cause if an unexpected action is taken by AI system. More transparent, explainable models of AI should be one of the future endeavors of AI basic science research. We need to establish interpretable

and understandable AI systems for users, which operates in a user-acceptable manner.

3) Improving security and robustness of AI system. In many cases, artificial intelligence system is designed to operate in a complex environment. AI system should be robust to deal with unexpected conditions and should be safe enough to cope with a wide range of intentional attacks. Before putting an artificial intelligence system into a wide range of applications, it is necessary to ensure that the system is safe, reliable and controllable. Lots of research endeavors are thus needed in the future to make AI systems more secure and robust, avoiding security accidents caused by malicious attacks and abnormal operation.

B. Strengthening Regulation on AI Development

The management of the usage of artificial intelligence is also important for handling the security, privacy and ethic problems of AI besides the technology research itself. Research on standardization, legislation and policy should be carried out to make sure that the application of artificial intelligence is in control.

1) Law & *Policy making.* Because the introduction of artificial intelligence may bring potential threats and risks, the governments can make laws and related policies to define what artificial intelligence can do or what is not allowed. Government needs to improve terms of laws and lay down rules for AI industry and products usage, such as the responsibility for the accident of unmanned vehicles, air UAV's invasion of personal privacy and so on.

2) Laying down standards. Because of the still preliminary stage of AI industrialization, there are no specific safety standards for many kinds of AI products, especially for robots that have the ability of moving, running and working frequently with humans. The rules and management are all urgent need for ensuring the security of AI applications. The future standards, recommended standards and other related documents should be updated periodically and the interval should be as short as possible, because artificial intelligence develops more rapidly than other techniques.

3) Management and supervision. We need to control and supervise the process of development of artificial intelligence because of its great influence. Google and many other well-known companies have set up an ethics committee to monitor the development and deployment of artificial intelligence technology. We must find ways to effectively monitor and review the AI systems in their applications. Many works still need to be put forward to promote the development of artificial intelligence while protecting human security and information security.

C. Improving Security and Privacy by Utilizing AI Technology

AI technology can also be used to protect our privacy, and enhance the security of systems. Not only the security level of our society and cyberspace, but also the individual privacy protection could be significantly improved with help of AI.

1) Enhancing cybersecurity. Cybersecurity has been recognized as one of the most complex threats to society. Artificial intelligence is regarded as a promising technology for cybersecurity defense. For example, Randrianasolo proposed an artificial intelligence based security system which has the ability to detect intrusion and learn to improve performance [10]. Sahil designed a user profiling system for cloud environment using AI techniques to enhance cloud computing security [11]. The further breakthroughs in knowledge understanding, representation, handling, and machine learning all will greatly enhance the cyber defense capability using latest AI methods.

2) Securing social life. There were studies showing that AI is a powerful supporting technology in policing, fighting crimes, cybercrimes, and enforcing law [12]. Your home security system can be equipped not only by facial recognition software, but also by biometric authentication sensors, from fingerprints, heartbeat and other features to identify identity. AI can be applied to detect attempted credit card fraud, and to conduct predictive analysis to prevent crime. Police can also patrol using unmanned aerial vehicle (UAV).

3) Improving privacy protection. We are in a world filled with private data, the promising trend of ubiquitous computing, such as location based services and radio-frequency identification, might violate people's privacy. Individual privacy protection must be addressed in order to guarantee the healthy evolution of information society. Many new AI techniques such as pattern recognition and machine learning could play important role in improving privacy protection by detecting privacy invasion behaviors [13]. The research on AI technology application in data desensitization, disclosure limitation and privacy invasion detection should be further encouraged in the future.

V. CONCLUSIONS

Artificial intelligence is developing at an exciting speed. The widespread use of AI technology can bring us efficiency and convenience, but we need to avoid harm to humans. Although wide range AI applications and their far-reaching impact have not appeared in our lives, it is necessary to discuss the social and ethical issues might be raised by AI in advance.

Emphasizing on security, privacy and ethic issues should be paid enough attention by AI researchers. The establishment of AI security norms and robots legal framework are inevitable problems for the development of artificial intelligence. In spite of the warning about the possible security, privacy and ethic threats, we believe that AI would help to bring us security. We can utilize the advantage of AI technology to improve the security and privacy protection for human society and cyberspace. With the development of AI, we strongly believe that this new technology is more likely to bring us benefit rather than harm.

AI is an emerging technology, and the regulation of it can't go too far. It is not advisable to carry out severe supervision on artificial intelligence especially at current application stage, so as not to build obstacles to technology innovation. On the other hand, it's very necessary to explore

the influence of AI to human society in various aspects, and to start to build up regulation systems progressively. Based on that, we can make best practice of AI application and greet a bright future with artificial intelligence.

ACKNOWLEDGMENT

This work was supported by research project "Research on China Artificial Intelligence 2.0 Development Strategy"(No. 2016GH010036) funded by the Ministry of Science and Technology of China.

REFERENCES

[1] D. Crevier, "AI: The tumultuous history of the search for artificial intelligence," Basic Books, London and New York, 1994.

[2] M. Flasiński, "History of artificial intelligence," Introduction to the History of Computing, Springer-Verlag New York Inc, New York, 2016.

[3] Executive office of the president of the United States, "The National Artificial Intelligence Research and Development Strategic Plan," Washington, October 2016.

[4] A. Pannu, M. T. Student, "Artificial intelligence and its application in different areas," International Journal of Engineering and Innovative Technology (IJEIT), Vol. 4(10), April 2015, pp. 79-84.

[5] S. S. Sikchi, S. Sikchi, and M. Ali, "Artificial intelligence in medical diagnosis," International Journal of Applied Engineering Research, Vol. 7, Jan. 2012, pp. 1539-1543.

[6] X. F. Hui, J. Sun, "An application of support vector machine to companies' Financial Distress Prediction," Third International Conference on Modeling Decisions for Artificial Intelligence (MDAI 2006), Tarragona, Spain, April 2006, pp. 274-282, doi: 10.1007/11681960_27.

[7] M. Kandlhofer, G. Steinbauer, S. Hirschmugl-Gaisch and P. Huber, "Artificial intelligence and computer science in education: From kindergarten to university," 2016 IEEE Frontiers in Education Conference (FIE2016), Eire, PA, Oct. 2016, pp. 1-9.

[8] P. Patil. "Artificial intelligence in cybersecurity," International Journal of Research in Computer Applications and Robotics, Vol.4(5), 2016, pp. 1-5.

[9] F. Kile, "Artificial intelligence and society: a furtive transformation," AI & Society, vol. 28(1), 2013, pp.107-115, doi: 10.1007/s00146-012-0396-0.

[10] S. A. Randrianasolo, "Artificial intelligence in computer security: Detection, temporary repair and defense," Ph.D. Dissertation, Texas Tech University, May. 2012.

[11] Sahil, S. Sood, S. Mehmi and S. Dogra, "Artificial intelligence for designing user profiling system for cloud computing security: Experiment," 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, July 2015, pp. 51-58, doi: 10.1109/ICACEA.2015.7164645.

[12] S. Alzou, H. Alshibly, A. M. Aitah, "Artificial intelligence in law enforcement, a review," International Journal of Advanced Information Technology, Vol. 4(4), Aug. 2014, pp. 1-9, doi: 10.5121/ijait.2014.4401.

[13] A. Solanas, A. Martínez-Ballesté, "Advances in artificial intelligence for privacy protection and security", World Scientific, Singapore, Aug. 2009.