2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress

Artificial Intelligence Cyber Security Strategy

Xiaohua Feng
School of Computer Science & Tech.
University of Bedfordshire, Luton, UK
Xiaohua.feng@beds.ac.uk
Tel. +441234400400

Yunzhong Feng
Hebei Normal University
Shijiazhuang, Hebei,
P.R. China
fyz02817@sina.com

Edward Swarlat Dawam
School of CST
University of Bedfordshire
Luton, Bedfordshire, UK
Edward.Dawam@study.beds.ac.uk

ABSTRACT

Nowadays, STEM (science, technology, engineering and mathematics) have never been treated so seriously before. Artificial Intelligence (AI) has played an important role currently in STEM. Under the 2020 COVID-19 pandemic crisis, coronavirus disease across over the world we are living in. Every government seek advices from scientist before making their strategic plan. Most of countries collect data from hospitals (and care home and so on in the society), carried out data analysis, using formula to make some AI models, to predict the potential development patterns, in order to make their government strategy. AI security become essential. If a security attack make the pattern wrong, the model is not a true prediction, that could result in thousands life loss. The potential consequence of this non-accurate forecast would be even worse. Therefore, take security into account during the forecast AI modelling, step-by-step data governance, will be significant. Cyber security should be applied during this kind of prediction process using AI deep learning technology and so on. Some in-depth discussion will follow.

AI security impact is a principle concern in the world. It is also significant for both nature science and social science researchers to consider in the future. In particular, because many services are running on online devices, security defenses are essential. The results should have properly data governance with security. AI security strategy should be up to the top priority to influence governments and their citizens in the world. AI security will help governments' strategy makers to work reasonably balancing between technologies, socially and politics. In this paper, strategy related challenges of AI and Security will be discussed, along with suggestions AI cyber security and politics trade-off consideration from an initial planning stage to its near future further development.

KEY WORDS

Artificial Intelligence (AI), Cyber Security, Data Governance, Strategy, General Data Protection Regulation (GDPR), Personal Identifiable Information (PII), Privacy, Trade-off, Deep Learning.

1 INTRODUCTION

AI cyber security are popular and useful scientific topic attracted many. Not only scientific researchers but also people in the world nowadays. The issues we shall face, not only pure science and technology problems around them, but also political and social influence challenges caused problems to our society. We shall demonstrate and discuss some of the relative challenges, which shown, there must be some compensations between the government and science or technology in most of the circumstances when strategic decisions are made (ICO, 2020). There are many current aspects and concerns related on AI security, some up to date exploration and discussions are reported.

2 BACKGROUND

The COVID-19 pandemic crisis has made many changes unexpectedly. Requirement to AI technology is one of them. AI security become not purely scientific or technical issues any more. It involves many unexpected aspects socially or even politically especially in government strategy making. Based on trends and concerns that already existed AI have developed further because of Covid-19 pandemic needs.

For instance, in UK robots are used to fight coronavirus. NHS (National health services) use AI technology on many applications. One of which is Robotics security related. Robot could do repeated work for nurses in nightingale hospital ward, or do many not complicated works with potential dangers for human beings. (i.e., A robot can help NHS and care homes to cure COVID-19 patients in many medical activities). While in robot security, ROS (Robot operating system) security is one of the key issues. Figure 1 represents an AI security example during a robot forensics investigation; i.e., a robot ROS forensics investigation procedure framework. Based on ROS features, these steps are: 1, Verification systems, (in other words, verify authentication); 2, Find out system description (for example, the vendor, version, serial number and so on); 3, Evidence acquisitions from the ROS and the (targeted system's) operating systems; 4, Timeline analysis; 5, Media analysis; 6, Data string or byte search; 7, Data recovery (and evidence analysis); 8, Reporting forensics investigation results. This

DOI 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00064

is distinct with a normal digital device's forensics investigation procedure due to the distinction of AI element characteristics in a robot from a parallel research with Abeykoon (2019). Another AI cyber security example is C2-ai–Precision Healthcare and Analytics. Copeland Clinical AI (C2-Ai, 2020) build an AI Applications in the cloud provides globally unique Ai-backed systems that AI technology with deep learning method have learned helping hospitals to reduce avoidable harm, mortality and variation.

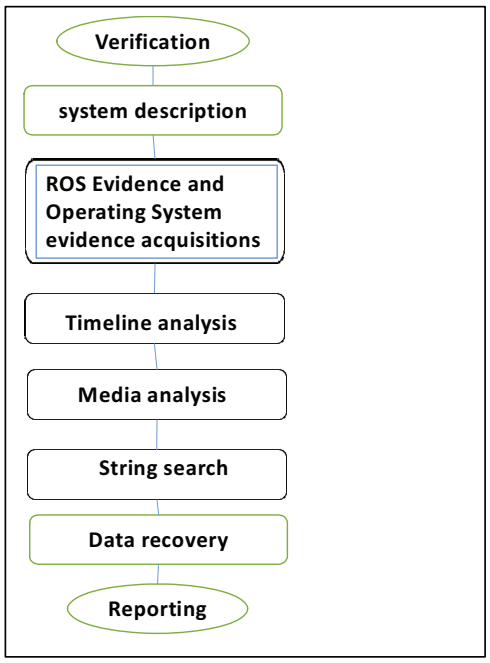


Figure 1 A security framework of ROS forensics procedure

Covid-19 use of proven security solution creating capacity now and resilience for the future and wont miss any urgent case. This means pre-emptively identifying and treating patients at greatest risk of developing HAP (hospital acquired pneumonia) and so on across NHS in UK. The compass Ai-backed SaaS tools of the cloud provide evidence-based clinical decision support prevention of avoidable harm. Cloud security grantee correct output. An evidentable demonstration for hospital resources.

Furthermore AI security example is in biometrics. For instance, a scan make use of AI deep learning technology to get into a pre-designed entry of property or information data control. Such as, enter a property, keyless car control, call center customer services, (like voice recognition software and automatic answering) systems. That saved many staff labor hours. Nevertheless, the security authentication is necessarily required for effectively access control. This kind of application is not avoidable to rely on security technology to ensure the AI application to carry on.

Personal privacy will be another dispute to be debatable. Westin (1967) defined privacy as "a claim of individuals, group or institutions to determine for themselves when, how and to what extent information about them is communicated to others". Another definition is, privacy is "the selective control of access to the self" (Altman, 1975; Margulis, 2003). In order to solve the current pandemic, test and trace or contact and trace are necessary. UK, Denmark, Germany, Italy, Latvia and Switzerland all use Gapple API (Application Programming Interface) app. In Pan-European Privacy-Preserving Proximity Tracing project, most states use Bluetooth Low Energy (BLE) as one of the choice, to save mobile phone in active state to distance measurement power consuming. However, in terms of enforced GDPR, personal privacy become a factor to one of the challenges. Besides, Bluetooth technique itself has many security threat to be consider; these are to be discussed later (ICO 2016; ICO 2020; Feng 2015). GPS could be another choice, but due to pitfalls of using inside buildings, at tube or metro and basement car park, also the insufficient precision issue. Therefore, its usage is limited.

3 The CHALLENGIES of STRATEGY

The global COVID-19 pandemic have made each of the government in the world have to make their own strategy from time to time, according to the pandemic changes. But, there are a number of challenges will influence the governments' decisions based on AI scientific result (NewScientist, 2017).

3.1 Technical Challenges

The first technical challenge would be the cyber security issue of AI technology itself. Since nothing could be perfect in a realistic situation. There is no chance to avoid any software using AI technology to produce unexpected flaw(s), like false positive. As mentioned previously, the consequence of the error could be potentially as serious as human being's life might be affected, that influence many governments' strategy makers to serve their citizens on the society. So if an AI prediction has not been securely processed, the result would be not trustworthy, the forecast data cannot be believed; even do not think of to be rely on

(Davey, 2020b). An article from the Guardian, Davey, Kirchgaessner and Bosely (2020) "Governments and WHO changed Covid-19 policy based on suspect data from tiny US company" is a typical example to show this kind of danger. With COVID-19 crisis, there has been little time for peer review and so on. For example, fake data from a company called Surgisphere was used in published papers (Davey, 2020a).

ROS cyber security is one of noticeable technical challenges as well. The Nightingale hospital demand staff labors to serve the crowded patients. A robot could help to share nurses' burden. However, precisely execute the doctor's treatment is necessary on security of lives (Abeykoon, 2019).

C2-Ai is another example of AI technology app. As the clouds dealing with its data process, the cloud security could possibly be a potential for its secure app result. Now, Detectify and Azure security tools can be used when take C2-Ai into account.

Biometrics cyber security could be even more important in the real world. Biometrics security is not only possibly has an impact immediately during the pandemic, but maybe also has an impact potential for these affected people's future daily life. Unlike the session security setting, AI biometrics authentication might last lifetime. Without appropriate law to protect, if this is revealed without consent, that could be like a time bomb threating for the lifetime to the person. Therefore, governments need to think very carefully to treat biometrics security as higher priory in their strategic planning.

Besides, the recent test and tracing trial project is working on contact and tracing app use AI and Bluetooth technology. During the trial, only gained about much less than predicted achievement on a few Apple mobile phone users when centralized way used. After testing and tracing trial, things could improve by make amendments to appropriate distributed contact and tracing app Gapple to local society. Initially, UK government were planning to using Bluetooth technique nationwide after success of their trial contact and tracing project. In fact, Bluetooth technology has many cyber security threats, such as, Bluebugging Bluejacking、Blueborne、Bluesnafing and so on. It should be used cautiously, following security best practice on app usage.

Furthermore, retraction made after Guardian investigation found inconsistencies in data, by US Company Surgisphere. (Davey, 2020b). The Lancet study had a dramatic impact resulted in the ends of the trial. It approved the importance of security as another case. It demonstrate, if the data security cannot be guaranteed, there is no valid AL forecast.

3.2 Some Non-technical Challenges

The social challenge, political challenge or in other words, non-technical challenge could be lively because of social reasons when strategy applied in the society during the pandemic crisis. Nowadays, our understanding of disease, transmission models and population scale health management are much more advanced, but the basic premise of contact tracing remains the same; i.e., to work out who infected individuals could have passed the disease onto, try to work out how, and act prevention to stop at least to limit the further spread. The contact and tracing trial face a private data owner, human right etc. issues.

The three stories had shown a conclusion

- in 1348, the black death was sweeping across Europe;
- in 1854, an outbreak of cholera in London as Dr John Snow researched (Levy 2020) and
- Mary Mallon, or Typhoid Mary's case in NY area around 1900-1907).

These cases are examples of contact and tracing being necessary for public (Levy 2020).

However, that is what the NHS contact-tracing app's aiming for, or help to do, by detecting and recording when people are near other app users and later telling you if you've been in 'high-risk contact' with someone who has symptoms. However, the app should have trustworthy security not to make the data incorrect misleading. As Hall (2020) described, one mobile phone app should safely and securely track those with whom you came into close proximity, and automatically alert you if any of them became infected with Covid-19 so you could get tested, or self-isolate (Hall, 2020).

The COVID-19 caused UK and other government use AI applications related with test and track. For example, Rekognition on face recognition (bbc, 2020a). Nevertheless, the recent global movement impaction caused society changes and chaos spread upon many countries in the world. That caused a number of consequences. For instance, Amazon, IBM, Facebook, Google, Twitter and some other companies had announced that they would stop to provide police use their products in the face-recognition application, until the house of lords or similarly law enforcement of other countries in the world have made new laws, such as, General Data Protection Regulation (GDPR), to monitor and manage this technology to applications. They have been supported by some communities globally. For example, TACL (The American Civil Liberties Union) in USA and so on (nytimes,

2020). These challenges are not only about technique aspects of cyber security and AI science itself alone but also much more than that. People need to have a broader overall consideration on other possible relevant surroundings impaction and consequences, which might possibly cause.

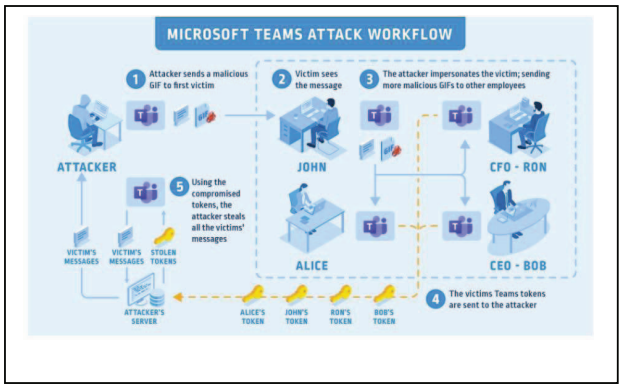
3.3 Privacy Consideration

On Cyber Law aspect, from legal theory of cyber science to some practical application (Holt, 2011), GDPR, Network Security Act, (Feng, 2019) E-Commerce Act and so on should be embedded to the test and tracing process, if possible. Otherwise that could result in human right issues.

In the June of 2020, take the COVID-19 pandemic into account, a trial project has been carried out at Isle of Weight with the support of local city council. The output is not as successful as the government desired. Only a few success have already reported it the process. Now an alternative AI software app has been adopted. If any trial project being taken into account nationwide, both Bluetooth security and PII personal privacy all need to be thinking of. Regarding privacy, people might have doubt in concern the human privacy when there is media publishes about spread, infection, to fighting crime, cyberbully, cyberstalking, cyber terrorism or government corruption. The fight against COVID-19 crisis is now presenting both the citizens and the government with new questions concerning about privacy in relations to health and economy, which become a concern that how should a privacy be managed in a global pandemic crisis period. Which is more important to compensate the economy of countries, and personal privacy of the citizens. Up to date, there is not any easier way to answering these kind of questions as it all depends on the individual's perspective and the scope of situation that poses and the circumstances occurring (Digital Health, 2020).

One of the COVID-19 pandemic's implications is that many people work from home. Microsoft Teams or Zoom video conferencing tools are the kind of the top productivity AI related applications during this pandemic period; even the British Prime Minister Boris Johnson also used Zoom for his cabinet meeting. However, there are reports suggested that there are security holes in collect and exchange information etc. The instant messaging among others can be used to promote advertising campaigns, like Google, Facebook and so on. The hosts could turn on 'attention monitoring' to test whether or not the audience is paying attention during the event (nytimes, 2020). Flaws have been consistently emerging. For example, a locational example is the Zoom or IoT app may meet the United State privacy standards; but, IoT and Zoom app do not meet the EU's (European Union's) General Data Protection Regulation (GDPR) (ICO, 2016, Eze, 2019). So does the Microsoft Teams similarly (Conor, 2020). IoT or Teams might let a third party to take over entire roster of the Microsoft Teams accounts, unfortunately as Figure 2 shown. In Figure 2, Conor (2020) has demonstrated an example of Microsoft Teams app personal privacy problem, which could be serious in terms of PII (Feng, 2015; ICO 2016). For instance. Privacy law questions have been asked similarly to about few incidence took weeks to inform its victims of a security breach. The UK's ICO (Information commissioner's office) and other states' data authorities were informed (bbc, 2020b).

Figure 2 Teams Security Issue (Conor, 2020)



Up to date, Johnson (2020) and others have analysis published. Repositories, dp3t-app-ios-ch, is a COVID-19 tracing client using the DP3T iOS SDK (software development kit) (Vaudenay, 2020).

3.4 A Good Trade-off Required

Summaries above, we can see clearly, a good trade-off between AI scientific data governance security and politics and social science are definitely needed when a strategy is made. There is no absolute perfect solution for all the issues during the crisis, governments have to consider good balance on all the problems arise. And deliver a good compensation in between. A security issue which relate to AI application could lead to problems with all the relevant strategy planning Further researches consider PII (Feng, 2015; Ali, 2020) are in progress at our University.

4 EVALUATION

As discussed the potential challenges above, AI services supply is in demand in many areas. All of these need information safety and security protection solutions to be considered, as well as PII data security law (Feng, 2015; ICO, 2016; Eze, 2019). AI science and technology security itself still has its own technical issue but have AI security is better than no security (Jain, 2006). Marx (2020) and Ali (2020) have some relevant exploration about NHS and cares (Liu, 2013) can explain. A government use of facial recognition technology can be ruled unlawful and violation human right by their court. Up to now, DP3T a Decentralized Privacy-Preserving Proximity Tracing tool could be useful in the trade-off. This repository documents a secure, decentralized, privacy-preserving proximity tracing system could be one of the solutions (Vaughan, 2020; Vaudenay, 2020). Further work still needs to be continued on follow privacy law under GDPR or equivalent.

Up to today, there is still without a thoroughly appropriate solution in the plan duration of the COVID-19 pandemic. For some of the outstanding cyber security issues to protect the online application and services. Professionals are all try our best to achieve a good trade-off between better online services and AI security in order to improve our society life styles. Currently, Amazon, Facebook, Google and IBM and other companies have stopped to provide AI face recognition applications software related with test and tracing and so on to the governments, which could have an impact on the contact and tracing plan to be considered.

5 CONCLUSIONS

Summaries above, we have explored the overall balance between AI and security technical solutions and government consideration for the society strategic opinions. Obviously, a reasonable better trade-off between science and technology with citizens' requirements should be in an urgent demand to be seriously treated. Now, deep learning AI technology can make algorithm recognizes various faces with higher accuracy. To control spread of the COVID-19, an application related with test and track such as Rekognition could be used on face recognition (bbc, 2020a). However, there are currently only a few laws restricting the use of facial recognition. The Coronavirus contact tracing app trial gets under way for good, that resulted in Amazon, IBM and other companies stopped supply to governments. Relevant new laws have urgently demanded to limit applications for good usage; and shown GDPR is closely followed. The research work being reported here is only an early stage exploration, still needs in-depth analysis based on investigation further internationally. Nevertheless, It is considered that the Kairos, FaceFirst, Ever AI,FaceFirst, Orbeus, Real Networks, Waldo, Kairos etc. apps and their companion companies need to take the GDPR and PII into account, to develop AI technology in terms of Law constrains. Fake data must be erased before publication (Davey, 2020b).

A recommended future development will be for a more appropriate approach to work out a better trade-off between AI and cyber security and the state's option. In order to get a better compensation in between citizens, government and commercial companies. It will deals with data acquisition with the multiple diversity issues, including GDPR and PII (ICO, 2016). DP3T could be one of the solutions now. Many researches on personal privacy and safety had been published in the past. (Feng, 2015; ICO, 2016; Ali, 2020). Furthermore, GDPR needs to be enforced for EU states and the related. Therefore, legal documents requirements should be as the top priority. Same to find a better trade-off between governments, citizen and AI & security organizations.

KEY REFERENCES

Abeykoon I. and Feng X. (2019) "*Challenges in ROS Forensics*", IEEE International Workshop ACE-2019.

Ali. J. and Dyo, V. (2020) "*Practical Hash-based Anonymity for MAC Addresses*". The 17th International Conference on Security and Cryptography.

Altman Irwin (1975) "*The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*" Brooks/Cole Publishing Company, 1975

Antoine Olivier, et al (2013) "*ISO 27018: The Future Standard for PII Protection in Public Cloud*" EBRC.

bbc (2020a) "*Amazon bans police use of facial recognition tech*". http://www.bbc.co.uk/news/business-52989128.
bbc (2020b) "*Blackbaud hack: More UK universities confirm breach*". https://www.bbc.co.uk/news/technology-53528329. [Accessed 10/06/2020].

C2-ai.net (2020) "*C2-Ai – Precision Healthcare and Analytics*" http//:c2-ai.net [Accessed 11/07/2020].
Conor Reynolds (2020) "*Microsoft Teams Vulnerability Let Hackers Take Over Entire Roster of Teams Accounts*". https://www.cbronline.com/news/teams-cyberark.

Coppin, Ben (2004) "*Artificial intelligence illuminated*", Jones and Bartlett Publishers, Inc; Computer ed. edition,

ISBN-10: 0763732303, ISBN-13: 978-0763732301.
Davey, M.; Kirchgaessner Stephanie and Boseley Sarah (2020a) "*Surgisphere: governments and WHO changed Covid-19 policy based on suspect data from tiny US company*" The Guardian, United Kingdom. 2020.
Davey Melissa et al. (2020b) "*Covid-19: Lancet retracts paper that halted hydroxychloroquine trials*", Guardian. https://www.theguardian.com/world/2020/jun/04/covid-19-lancet-retracts-paper-that-halted-hydroxychloroquine-trials.

Eze, E.; Sant, P; Zhang, S; Feng X. & et al. (2019) "*Mobile Computing and IoT*: Radio Spectrum Requirement for Timely and Reliable Message Delivery over Internet of Vehicles (IoVs)". Springer, ISBN 978-3-030-374679.

Feng, X. and Zhang X. (2015) "*Personally Identifiable Information Security in Cloud Computing*", International Conference on Computing and Technology Innovation, UK

Feng, X.; Feng Y. and et al. (2019) "*Computer Laws Consideration on Smart City Data Planning of Chongli*". IEEE Xplore 2019 Smart City Congress, ACE-2019, UK.
Feng Y. (2011) "An Investigation and Study on the Situation of Diving Reserve Talents in Human Capacity Building of Sports Industry"

Hall Kathleen (2020) "*Where-is-matt-hancocks-contact-tracing-app*". The Bureau of Investigative Journalism.

Holt Jeremy et al. (2011) "*A Managers Guide to IT Law*", British Computer Society, 2nd Ed. ISBN: 1906124752.

Hurbans Rishal (2020) "*Grokking Artificial Intelligence Algorithms*", 28 Nov. 2020, Manning (28 Nov. 2020), ISBN-10: 161729618X, ISBN-13: 978-1617296185.

ICO (2016) "*Overview of the General Data Protection Regulation (GDPR)*". ICO: Information commissioner's office. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ [Accessed 14/06/2020].
ICO (2020) "*Data protection and coronavirus - what you need to know*" ICO: Information commissioner's office. https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/

Jain A. (2006) "*Biometric Authentication*" https://ukdiss.com/litreview/biometric-authentication-literature-review.php [Accessed 22/06/2020].

Johnson, G.A.; Shriver, S.K. and Du, S. (2020) "*Consumer privacy choice in online advertising: Who opts out and at what cost to industry*?" CU Experts, Marketing Science, 1.

Ladley John (2012) "*Data Governance*", A volume in MK Series on Business Intelligence, How to Design, Deploy and Sustain an Effective Data Governance Program, Elsevier Inc. ISBN 978-0-12-415829-0

Levy, Ian (2020) "*The security behind the NHS contact tracing app*", National Cyber Security Centre. https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app [Accessed 14/07/2020].

Liu E. & Feng X. (2013) "*Trustworthiness in the Patient Centred Health Care System*", Springer, Berlin Heidelberg.

Margulis, Stephen T. (2003) "*Privacy as a Social Issue and Behavioral Concept*", Journal of Social Issues, Vol.59, no.2 https://doi.org/10.1111/1540-4560.00063, [Accessed 18/06/2020].

Marta Rybczyńska (2020) "*Open-source contact tracing*", June, 2020 https://lwn.net/Articles/823532/
Marx, M., Zimmer, E., Mueller, T., Blochberger, M. and Federrath, H. (2018) "*Hashing of personally identifiable information is not sufficient*". SICHERHEIT.

Merrick Robert (2019) "*Data Privacy Governance in the Age of GDPR*", Risk Management magazine.

New Scientist (2017) "*Machines that Think: Everything you need to know about the coming age of artificial intelligence*". ScienceDirect.

New York Times (2020) "*England's World Beating System to Track the Virus Is Anything But*", New York Times, US.

Patterson Josh and Gibson, Adam (2017) "*Deep Learning: A Practitioner's Approach*", O'Reilly Media, ISBN 9781491914250.

UK government (2019) "*Biometric recognition and authentication systems*", UK.

Vaudenay, S. (2020), "*Analysis of dp3t*", Between Scylla and Charyblis. EPFL, Lausanne, Switzer.

Vaughan, A. (2020), "*The problems with contact-tracing apps*". New Scientist 246(3279).

Westin, A. F. (2015) "*Privacy and Freedom*". Ig Publishing, ISBN-10: 1935439979.
Westin, Alan F. (1967) "*Legal Safeguards to Insure Privacy in a Computer Society*", Special Report, Columbia University, New York USA.