THE DARK SIDE OF INDUSTRIAL REVOLUTION 4.0- IMPLICATIONS AND SUGGESTIONS

Khalid Rasheed Memon, Universiti Sains Malaysia
Say Keat Ooi, , Universiti Sains Malaysia

ABSTRACT

The buzz word, "Industrial Revolution 4.0," has acquired immense popularity among research scholars these days. Several papers have been published on the optimistic side of the subject under various headings such as cyber-physical systems, the internet of things, smart technology and the digitalization of industrial manufacturing, etc. However, scarcely have researchers touched the negative or dark side of such a drastic technological paradigm shift, leaving a huge gap in the knowledge body. As a result, very little is understood about the negative effects of the industrial revolution 4.0. Our article highlights the potential disadvantages/negative effects of the industrial revolution 4.0, so that researchers and professionals can proactively prepare and devise measures that recommend the regulatory system or control-mechanism required to prevent significant expected fatalities in the future. Our research presents responsible research and innovation as a solution for the management of IR 4.0 disasters.

Keywords: Industrial Revolution 4.0, Cyber Physical System, Big Data, Cloud Computing, Cyber Security And Crimes, Artificial Intelligence, Responsible Innovation, Business Ethics.

INTRODUCTION

The fourth industrial revolution *i.e.* IR 4.0 is leading the world to a newer phase of industrialization and technical innovation. It will be dominated by the use of cyber-physical-systems and internet of things and Services & cloud computing in manufacturing and industrial processes. (Zhong et al., 2017; Sung, 2018; de Sousa Jabbour, 2018) Drastic changes are going to occur all over the organizations with respect to their influences on value creation, business model of the company or downstream services. Bartodziej, (2017) In fact, IR 4.0 is nothing more than an extension of information and communication technology (ICT), combined with the exponentially grown transmission, computing and storage that is enabling the materialization of extremely powerful, interconnected technological systems, the "Cyber-Physical-Systems".

Piccarozzi et al., (2018) define cyber physical systems as "systems that integrate computation, networking, and physical processes and include a multitude of technologies that involves mobile devices, the internet of things (IoT), artificial intelligence (AI), robotics, cyber security, and 3D printing". The definition describes that IR 4.0 would have an impact not just on industrial production but also on our everyday lives. Now it has become common to interact with robotics and artificially intelligent devices Ekudden, (2018) such as 3D printing, home health examinations, educational learning agents, online car sales systems, gaming & entertainment, maintenance and so on (Winfield & Jiroka, 2018; Piccarozzi et al., 2018). Our small and medium-sized businesses will also be significantly influenced by this technical advancement and the fusion of virtual world with physical world that has become feasible; thanks to these cyber physical systems (Wang & Wang, 2016).

A cyber physical system make it possible to have access to the information & services anywhere, including in your hands, and it is not complicated in today's era of networking. We all use smart-phones, vehicles and home appliances, whereas they can be remotely controlled. Take the example of air conditioning, for example, from which you want to turn on the cooling machine when you're on your way back home, and you want your room to be cold. Coffee machines will even make coffee for you when you're in bed to save the waiting time. In addition, remote access may be required for the repair of these machines, which may help to locate the real issue and to provide the service personnel with the correct spare component. Even its system can order the required spare parts for itself by means of an appropriate communication infrastructure (Jazdi, 2014).

Apparently, IR 4.0 has all the positive attributes that can make manufacturing autonomous and smart, scalable, accurate, efficient and sustainable by its intelligent systems (Wang & Wang, 2016; Muller et al., 2018). Furthermore, IR4.0 and cyber-physical devices deliver tremendous social advantages in virtually every walk of life by conducting activities on their own (through robotics), can minimize costs and time without human effort, providing service standardization and can support humans with menial and hazardous tasks (Muller et al., 2018). We're going to get self-driven cars, when the whole society's automation is going to be the next step (Cath et al., 2018)

However, due to the industrial revolution 4.0 and related technologies, the world may face horrible consequences, particularly by means of artificially intelligent machines/robotics. It is predicted that these artificially intelligent super machines and computers will go beyond the human race in all walks of life between 2020 and 2060, though renowned scientists and technology experts such as Bill Gates, Elon Musk, Steve Wozniak are alert and calling it a great danger to mankind in the coming days. (Helbing et al., 2019; Dreyer et al., 2017). Further, Big data and artificial intelligence are need of the time and the advantages of these AI technologies are immense, but abuse of data for own gain, exploitation of minds for political benefit and billions in earnings is not acceptable. It is also against basic human rights and a direct violation of its principles (Helbing et al., 2019). There are many cases of data leakage, surveillance and privacy, as explained by Pigni et al., (2018). The authors Pigni et al., (2018) elucidate that about 87% of U.S. residents can be identified by their 5-digit zip code, date of birth and gender only. Due to such quick access to the data, roughly, three million (3 million) records were hacked per day in 2016, although this number is rising at a rate of 15 per cent per year. Data breaches in North America accounted for the majority of all data breaches and accounted for 80 per cent of the world's overall data breaches. Also Europe is not protected and accounted for 10% of the total infringements and stolen records, while Asia and the Pacific region accounted for 8% of the world's total infringements. Pigni et al, (2018) It is now becoming clear that data protection and privacy and the avoidance and limitation of abuse and unwanted access are now one of the most serious issues (Alcacer & Machado, 2019; Sun et al., 2014; Liu et al., 2018; Liao et al., 2017; Horváth & Szabó, 2019).

In general, technological innovations are considered to be beneficent for the society, but on the contrary to this, due to IR 4.0, we'll lose our democracies, our autonomous and self-governing decision making and our distinction therefore we need to safeguard these bases of our livelihood since these are the basis of our success and greater efficiency. Helbing, (2019) In fact, being mature information societies, we must be well prepared and have planning for such technological innovations having social, ethical and economical and sustainability impacts. Such digital transformations should not come to us in a sudden and unexpected way Cath et al., (2018), however, till yet rarely authors have written on the dark side *i.e.* the threats and

disadvantages of IR 4.0 and thus there is huge gap on this subject (Piccarozzi et al., 2018; Muller et al., 2018; de Sousa Jabbour et al., 2018; Horváth & Szabó, 2019) Most of the authors have only focused on defining IR 4.0 and its technologies, its benefits and technological advantages to the industry and society, resulting in leaving behind the need and gap to highlight the negative consequences of IR 4.0.

Our research would specially focus on the single research question that "what potential threats and harms can IR 4.0 and its technologies cause to our industry and society"? Accordingly in the below sections, we would discuss what exactly IR 4.0 is and then the potential harms and negative consequences in detail, which can be resultant of IR 4.0 and its components or cyber physical systems. Further, it will end discussing the practical implications, future research & limitations and conclusion, while summing up the paper and proposing some measures. However, it should be noted that its perspective article, based on our own analysis and research and may differ from others perspective and research.

What Exactly is Industrial Revolution 4.0?

Industrial revolution 4.0 is about bringing revolutionary change in manufacturing technologies. It was initiated by Germans as strategic move aiming to create intelligent manufacturing units based on cyber physical systems, internet of things and cloud computing. Zhong et al., (2017). However now other countries like U.S, China, most of Europe are working on it and have inculcated this in their long term and strategic planning so as to strengthen their manufacturing processes and advance service innovation. IR 4.0 is all about introducing internet and related technologies in manufacturing processes whose main aim is to make industries more intelligent, resource efficient, adaptable and ergonomic (Wang & Wang, 2016). It got started from the Hannover Fair in 2011 and thus since then it has gained tremendous attention and focus all over the world by all segment whether academicians, politicians, government officials etc (Sung, 2018).

It's basically integration of technological innovations like cyber physical systems, internet of things, cloud computing etc and their use throughout the manufacturing as well as logistics processes. These technologies will introduce completely new and novel ways of dealing all the processes, creating a flexible, self-organized and decentralized production system instead of previously used humanly controlled, centralized and classical approach (Bartodziej, 2017). Kagermann et al., (2013) defines IR 4.0 as "Industry 4.0 represents nothing less than the fourth industrial revolution, comprising 3D printing, Big data, Internet of Things, and Internet of Services, *i.e.*, all the ingredients needed to facilitate smart manufacturing and logistics processes". The authors Liao et al., (2017) consider the final report of the Industry 4.0 working group Kagermann et al., (2013) as the most recognized & renowned Industry 4.0 reference due to its citations and discusses the three essential integration features of IR 4.0 as "Horizontal integration", "Vertical integration" and "End-to-End digital integration". The authors Kagermann et al., (2013) explained these three integration features as following:

Horizontal Integration

"The integration of various IT systems used in the different stages of the manufacturing and business planning processes that involve an exchange of materials, energy and information both within a company (e.g. inbound logistics, production, outbound logistics, marketing) and between several different companies (value networks)"

Vertical Integration

"The integration of the various IT systems at the different hierarchical levels (e.g. the actuator and sensor, control, production management, manufacturing and execution and corporate planning levels) in order to deliver an end-to-end solution".

End-to-End Digital Integration

"Integration throughout the engineering process so that the digital and real worlds are integrated across a product's entire value chain and across different companies, whilst also incorporating customer requirements". Industrial revolution 4.0 should be considered as "Smart thinking" approach which would have effects on every walk of life along with industries and manufacturing processes. It will transform our lives to a new era of digitalization where everything would be expected to be smart like smart cities with respect to self-sustainability, energy supply, resources, logistics and mobility solutions. With regards to the manufacturing processes, this technological revolution would make production processes to be upgraded at intelligent level by virtue of which decision will be taken dynamically for the resolution of the problems. Through the usage of artificial intelligence, these machines would learn by itself from previous experiences so as to reach at the optimum level of production and reaching the ultimate pathway for any specific product's process and industrial practice Zhong et al., (2017) This would be made possible through the extensive usage of complex computational techniques, information and communication technologies, various devices like sensors, actuators, modern manufacturing technologies, intelligent devices, data analytics and their embedding. This embedding would enable highly intelligent human-machine manufacturing system whereby human interaction/involvement can be decreased due to the use of intelligent manufacturing system (Zhong et al., 2017).

Framework Model of "Industrial Revolution 4.0" for our Research

Our research would focus on four components of below presented model in Figure 1, plus one additional area affecting overall society/world, and are presented below:

- Cyber Security *i.e.* data security and privacy issues
- Big data
- Cloud computing
- Autonomous robots *i.e.* super intelligent machines or computers in coming era.
- Effects on "Job" and "Employment" (Additional societal issue)

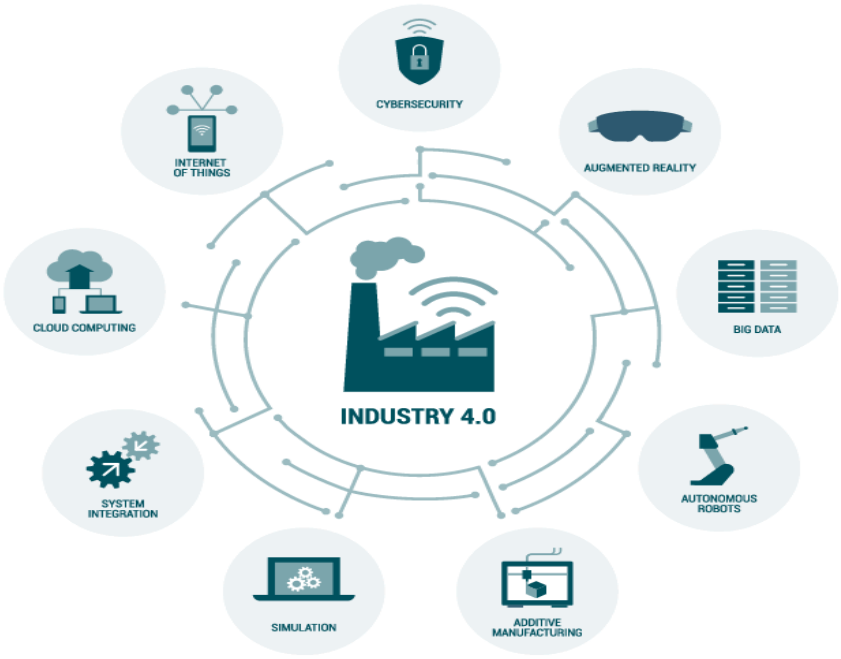

FIGURE 1
FRAMEWORK MODEL OF INDUSTRIAL REVOLUTION 4.0 GRAPHICALLY REPRESENTED BY I-SCOOP LTD BASED ON (WANG & WANG, 2016)

In our opinion, these four components of IR 4.0 plus one additional area (job & employment) would seriously affect our industries, society and world. Therefore, we'll present our perspective and analysis as per our research and will discuss their drawbacks, effects; threats to the society in the next section. Also, they will be defined in their relevant sections.

Dark Side of Industrial Revolution 4.0 Through Its Components

This section comprises of the analysis, implications and brief suggestions regarding IR4.0 and its components as per our perspective and analysis based on the model presented in Figure 1 and section 3.

"Big Data" and Its Disastrous Impacts

Big data is being used everywhere now a day, however, concept wise, 'big data' can be considered as embryonic and has doubtful origins (Bihl et al., 2016). The authors Wang et al (2018) considers "the term "big data" was used for the first time in 1997 by Michael Cox and David Ellsworth in a paper presented at an IEEE conference to explain the visualization of data and the challenges it posed for computer systems" whereas Gandomi & Haider (2015) convey that Diebold (2012) argues that the term "big data . . . probably originated in lunch-table conversations at Silicon Graphics Inc. (SGI) in the mid-1990s, in which John Mashey figured prominently". However, the term got well known at later stages like during 2011.

A stream of researchers has suggested and agreed upon the three dimensions for understanding the concept and handling the challenges with regards to big data. These are three V's (Bihl et al., 2016; Gandomi & Haider, 2015; Kwon et al., 2014; Wang et al., 2018) which

are: 1 Volume 2) Variety and 3) Velocity. Although, some researchers suggest upto 7 V's, however, the consensus cannot be made on them due to industry specificity; yet these three V's are the common attributes of all those V's (Gandomi & Haidaer, 2015). The three dimensions can be explained further, for instance "Volume" may be considered as huge magnitude and quantum of data *i.e.* data in 100s of terabytes & peta bytes. "Variety" refers to various data forms or heterogeneous structures like text, audio, video, images. "Velocity" can be understood with regards to speed *i.e.* the rate at which data is received, stored, processed and analyzed, specifically with reference to the streaming of data, in real time and near to real time (Gandomi & Haider, 2016)

So, how the digital world will change the whole world? It's in full swing now. We are producing lot much data every year through our Facebook posts and hundreds and thousands of every minutes' Google searches and also through the usage of Google Maps for seeking direction towards desired destination and so on. Around 700,000 queries are sent to Google and 500,000 comments are sent at Facebook, in just a minute. Whereas data produced on other various applications and media is enormously big, due to which our produced data is getting doubled every year. It means, our produced data in 2019 is the double of our entire history's produced data till 2018. (Helbing et al., 2019; Helbing, 2019) and by the way what do we do in our posts? We share our feelings; information related to how we think. Every minute and single activity of ours is being recorded and noted. The same can be observed practically by visiting my activity @ google.com. You will find every single web page you opened, your browsing history, your favorites which you visited most and so on. Nothing is hidden now. Similarly, CRM softwares of various websites are tracking your activities and then they present to you some options which may be suitable as per your likeness tracked by the artificially intelligent applications. They present personalized advertisement and discounts to manipulate your minds and choices and even play with people's feelings since they are aware that how you respond to certain situations. These applications are more aware about us than our friends and often they give us the choices as those were ours, although we have not chosen them.

Singapore and China are the perfect examples of today's data-controlled societies. All those activities which were harmless earlier have become problematic now. For instance, a program in Singapore was started to protect its residents from terrorism whereas now it's directed towards influencing immigration and economic policy, school curricula and the property market. Similarly, in China, a project named China Brain was initiated by Google for the military which involves execution of purported profound learning algorithms and data was collected over the search engine about its users. But what happened later on? Recently reported, the same application is being used for the monitoring of their citizens activities through a so-called scoring program by virtue of which every Chinese citizen will get citizenship score that will establish the eligibility as well conditions for taking loan, travel visa to other countries as well as jobs. Whereas the wrong choice as per the government would give you negative consequences while abolishing the citizens own choice and autonomy (Helbing et al., 2019).

But this would not stop here since the world is moving towards "persuasive computing" which would manipulate our minds through the use of sophisticated algorithms on our data and we would be steered through free internet offerings or complex work processes; even these would be used in politics as the governments like to steer their citizens. Especially during elections, whosoever will control and use this technology for the manipulation of undecided voters, can win the elections whereas the said controlling of minds would be difficult to detect (Helbing et al., 2019).

One of the major and recent data scandals "The Facebook–Cambridge Analytica data scandal" is an example of such incidences. It was a kind of political scandal of 2018. And it was exposed that Cambridge Analytica had gathered the personal data of millions of facebook users from their profiles without their permission and used it for political promotion purposes. Although, Mark Zukerberg, the owner and director of Facebook, apologized later on and pledged to make changes in data protection and privacy reforms so as to avoid such breaches in future, yet the scandal incited a debate regarding the ethical standards for greater consumer protection and rights on similar media.

Big data and artificial intelligence are need of time and there are enormous benefits of these AI applications however, the misuse of data for own benefits, manipulation of minds for political benefits and earnings of billions is not acceptable. Even it's against basic human rights and a clear violation to its principles (Helbing et al., 2019). There should be some principles to be based upon and we need to strive for its regulatory framework and implementation. And thus, we can get guidance from researches in the areas of "Responsible research and innovation" (RRI) and this big data can be used for social good i.e. to harness the social problems like poverty, disease, hunger, crime, economic, human rights and social inequality (Bean, 2016).

Cyber Security (Data Security & Privacy Issues)

The term "Security" has been defined as "a process to protect an object against physical damage, unauthorized access, theft, or loss, by maintaining high confidentiality and integrity of information about the object and making information about that object available whenever needed" Abomhara, (2015) whereby the security requirement of general ICT systems and IoT environment is just the same. Today, the security and privacy of data and to create prevention and restriction on the misuse and unauthorized access is becoming one of the greatest issues (Alcacer & Machado, 2019; Sun et al., 2014; Liu et al., 2018; Liao et al., 2017; Horvath., & Szabo., 2019) since this has become the source of earning billions. Due to lowered business ethics, business partners or third parties may take advantage and misuse each other's data through unauthorized access. Internet of things and related technologies are expanding but they are spreading fear as well whereby control over huge collected data is the most disturbing aspect (Roblek et al., 2016). Even the real users of internet do face greater problems with regards to security and privacy issues. In general, home routers can easily be invaded whereas data can be stolen, deleted and changed. Regarding privacy, those data providers who render free mailboxes, navigation, calendars, storage and other several applications are really questionable since we don't know where these operators can sell our documents. Following are the major issues in this regard:

- Exposure of personal information
- Cyber-attacks and fear of financial/secret data stealing
- Highly sophisticated tools used by cyber criminals

It seems that Industry 4.0 will expose maximum personal information the world has ever seen. Several recent incidents of information leakages have stunned the world with regards to data privacy for instance the data breach of Target Inc which was 100 million dollar data breach, whereas other bigger firms being victims of such data breaches include American Express, Ali Express (working under ownership of Alibaba.com), JPMorgan, The US Postal Service even SONY Pictures etc, (Pigni et al., 2018). The authors Pigni et al., (2018) explains that around 87%

of US citizens can be identified by their 5-digit zip code, birth-date and gender only. Due to such easy access to data, approx. three million (3 million) records were stolen per day in 2016 whereas this figure is increasing with the rate of 15% every year. The data breaches in North America accounted for the largest of all data breaches and were 80% of the total world's data breaches. Even the Europe is not safe and it accounted for 10% of total breaches and stolen records whereas Asia and Pacific regions got 8% of total world's breaches (Pigni et al., 2018).

The author Abomhara (2015) argues that cyber threats can cause severe financial damages and losses to the users. After the emergence of IoT, everyone whether corporate sector, public sector or a simple home computer user, have become vulnerable to security problems. The attackers can take control over the air-conditioning, heating or even physical security systems which were automated for personal ease/safety. The information can be sought through sensors embedded with these systems and attacker can easily know your presence or absence at home. Even the attacker can take photos, track locations, record your conversations, take control of your smart phone, make calls, use your camera and microphone etc (Ali, & Awad, 2018). Similarly, cyber-attacks over public utility systems could be made for the stopping of water supply and electricity to residents (Abomhara, 2015). Thus, it must be understood that the cyber-criminals are constantly working on the advancement of their skills, tools and techniques whereas the software and technologies we generally rely, also change and get updated so we need to update and apply patches, use all kind of measures including anti-malware tools, firewalls and so on. Further we must be very watchful and keen regarding the use of holistic approach for the prevention of such threats rather than focusing on detection only. Security is not available for free and those avoiding investing amount on such sensitive issue, will have to bear heavy loss due to the avoidance of this extremely critical cost.

Ali & Awad (2018) have suggested some counter measures for "IoT based smart homes" which may be applied to smart industry as well since security requirements are just the same. These include the use of bio-metric identifiers like finger prints, retinal scans, hand geometry, iris patterns and signatures. These can be used for hardware platforms as well. In this regards, multifactor identification mechanism (use of two or more identification claims) is suggested along with the continuous awareness programs and trainings on security and privacy issues. Further, secure Wi-Fi connections within smart factories/homes can prevent the hijacking of network link and serve the security / safety purpose, whereby the services of only authentic IoT devices providers may be sought. Additionally, soft access of data as well as the physical access to all system devices & their configurations may be restricted to very limited & authorized users only (Ali & Awad, 2018).

Issues with "Cloud Computing"

The industrial revolution 4.0 is mainly based on cloud computing whereas consumers around the world are still reluctant to adopt the same due to various security risks and concerns (Kaufman, 2009; Takabi, et al, 2010; Chen & Zhao, 2012; Sun et al., 2014; Liu et al., 2018). Cloud computing offers two products over the internet environment 1 Applications i.e. software to perform relevant tasks and 2 Resources i.e. storage and virtual machines (Sun et al., 2014). Although lot much is claimed about the security and privacy of cloud computing yet it's not as safe as it is being claimed. The authors Chen & Zhao (2012) have described the security and data leakage events as proof of vulnerabilities and threats for data. These events took place in biggest companies like Amazon, Google Docs, Google Gmail and Microsoft's Azure cloud computing. They faced different tricks like stoppage of services, leakage of data even user's private info etc.

however, it should be noted that these are the companies who are providing the most of cloud computing services (Sun et al., 2014). Thus, a data breach in cloud computing is an illegal or unauthorized access to data hosted within the cloud, with regards to both retrieving and modifying data. Within cloud computing, such data breaches are considered as particular concerning issue by virtue of which firms loses its sensitive information like trade secrets or details of some very sensitive, big and profitable contract, resulting in the development of firm's negative reputation (Esposito et al., 2016).

In fact, the cloud computing functioning is like having multiple tenants which may include some weaker tenants having lesser security privileges & needs or financial constraints of affording the high-end security or due to any other reason. Thus, the security in cloud computing becomes as strong as the weakest link/tenant in its network. If, that weakest link is traced, then it can become easy target for cyber-attack due to which the other tenants in cloud may be in the same danger like the first one. (Kaufman, 2009; Chen & Zhao, 2012) On the other end, privacy is also at stake for both customers and producers. Customers' data will be collected and analyzed for which customer may be seriously concerned. This is not the only case here instead due to inter connectivity the same problem persists between small and larger companies or the suppliers who never like to share their data. Accordingly, there is great challenge to work transparently and reduce the gap among consumers and producers (Martin, 2017). Thus, there is great need to develop a "Trust-based data security framework" (not in scope of our article) which should involve the policies regarding access of data of trustees, values, dynamically altering security needs of trustees, based on inter-domain and cryptographic algorithm, homomorphic or asymmetric encryption (Sun et al., 2014; Chen & Zhao, 2012). Chang & Ramachandran (2015) has also suggested a good architecture and framework titled as "Cloud computing adoption framework" and that may be referred for further details. Data security and privacy is mandatory requirement since the organizations cannot survive in such an unsecure data vulnerability environment specially the SMEs who do not have their own private network and hi-tech organizations which are likely to adopt cloud computing technology.

Super-Intelligent Machines Vs Human Beings

The artificial intelligence field is now growing exponentially. Gone are the days while programming was written as line after line. Now everything is going to become intelligent. We'll be having smart homes; smart cities and smart industries in upcoming era (Helbing et al., 2019). The scientists are working on transforming the human attitude in robots; however, as a matter of fact, these AI machines are more intelligent than humans in number of grounds for instance, in calculations, driving vehicles, playing chess and strategic games etc. Further, these self-learning robots are building themselves through their self-learning abilities so there's not much time left that smarter machines than human are developed. Earlier researches in AI during 1950s were focusing on the areas like problem solving & symbolic methods whereas during 1960s, the US Defense department took interest and trained these machines to imitate reasoning skills like human. These basic steps opened the way towards more research and efforts to work on this field resulting in today's computers which assist us as decision support systems (DSS) and smart computers etc. However, till today the scary picture of these robotics is still a science fiction, although this may happen in future if we didn't regulate or formulate suitable strategy to control and configure technological innovations yet we can prevent it before happening.

It is expected that these artificially intelligent super machines and computers will go beyond human race in every walk of life between 2020 & 2060 whereas the renowned scientists

and technological specialists like Bill Gates, Elon Musk, Steve Wozniak are warning and considering it great danger in the coming days for humanity (Helbing et al., 2019).

Further, these artificially intelligent machines can be used irresponsibly and in a potentially harmful way for the achievement of evil causes and thus they can be more harmful than atom bomb (Winfield & Jiroka, 2018). Power is always attractive and needed by criminals, terrorists and extremists. There is no guarantee against robotics misuse since the hackers had even hacked the computer systems of Pentagon and American White house. Helbing, (2019) Therefore, it is advised to develop collectively distributed intelligent machines instead of building such super intelligent and powerful machines which become uncontrollable.

Effects on "Job" and "Employment"

There are serious concerns in public regarding jobs and huge unemployment Winfield & Jirotka, (2018) even fear of further de-industrialization (Dombrowski & Wagner, 2014). Industrial revolution 4.0 will obviously change the job roles (Muller et al, 2018; Horváth & Szabó, 2019) and may require more thought provoking but less technical or professional skills oriented, problem solving, self-organizing work tasks and competencies. (Kiel et al., 2017; Dombrowski & Wagner, 2014; Frey & Osborne, 2017). It is claimed that the aim of cyber physical system and smart manufacturing is not the substitution of human with machines instead the interconnection and collaboration of human and machine is desired to obtain mass customization through their synergetic effort. However, low skilled jobs and technical personnel with routine jobs, will become un-employed and get substituted by artificially intelligent robots. (Kiel, 2017; Frey & Osborne, 2017; Horvath & Szabo, 2019) Accordingly, the mental requirements would get increased for the employees specially related to work system and process orientation and the jobs requiring expert planning and monitoring will be in demand (Kiel et al., 2017; Dombrowski & Wagner, 2014) since the machines would be able to predict problems themselves and rectify the issue even before its occurrence without any intervention of human hand Lasi et al., (2014). However, till today, there is ambiguity regarding the required qualifications and competencies of worker (Muller et al, 2018a, Kiel, 2017) even managers would need more skills so as to interact with machines and cope with the new era's demands and challenges (Piccarozzi et al., 2018). Therefore, research scholars and practitioners should also focus on this area and highlight the shortage competencies and skills for building up our industries in those specific areas (Kiel et al., 2017).

For everyday life, consider if there would be self-driving cars then who will need drivers to hire? Similarly, typing jobs, newscaster job, filing clerks, bank tellers and other so many routine jobs will be replaced by robots since these jobs can be done by robots easily and even better than human. Robots don't get tired, for instance, a single robot can read news for 24 hours or can type for 24 hours without getting breaks or changing shifts. Therefore, it would replace human in routine jobs. However, jobs related to social interaction, consultation, physical examinations in medical care, creativity, technical jobs (e.g. plumbers, pipefitters), judges & magistrates and thought provoking or critical thinking jobs will be performed by humans since these are not computerize able (Frey & Osborne, 2017).

Future Implications and Suggestions

We have discussed in detail the impacts and harms that industrial revolution 4.0 can cause to our world. Although, technological improvements are much needed and required for the

benefit of humanity yet the mechanism for controlled use of such technological innovations should be developed to avoid any mishap in coming days. Several future implications have been discussed between the lines in detail to make it clear that in general, innovations are considered to be beneficent for the humanity, however; all innovations are not responsible innovations. Here we would present future implications in a bit different manner i.e. the problems which should be avoided but these are occurring and may create panic situation in coming future:

Problems: Technological innovations:

- Should be for the benefit of mankind rather hazardous.
- Should be socially desirable, ethically & cognitively acceptable and sustainability oriented.

- Should generate profits for the business.
- Should be inclined towards value creation/enhancement.
- Should be controllable and manageable. Should not be more powerful than human being.

In addition to these problems there should be regulatory framework to handle these issues as well provide support to business organizations whereas decreasing governmental resources and increasing the power of private companies are the reasons that regulations have become difficult to implement or regulations have not even been made. It has become challenging to control these technological companies. Research scholars have presented different suggestions and solutions to addressing these issues, for instance, the authors Guihot et al., (2017) have proposed two ways to handle such situation 1) Nudging and 2) Interacting and participating with the technological companies. However, we present our opinion in the form of following possible solutions:

Solution: Technological innovation organizations:

- Should now discuss technology in terms of benefit as well as risk for all mankind.
- Should focus on input and process rather just focusing on outcome part.
- Should have governance mechanism at input and process parts ensuring the production of humanitarian products.
- Should establish a mechanism by virtue of which they involve and engage its stakeholders to develop and maintain trust regarding complete production/innovation process. This mechanism is required to ensure cognitively and ethically acceptable, socially desirable and sustainable customized product.
- Should be learning organization having continuous improvement system with regards to future technological needs & requirements as well as other issues pertaining to technological innovations i.e. responsive and adaptive to change.

Thus, there are greater challenges and higher uncertainty of the future impact of the technological innovations such as those in biotechnology and nanotechnology (the current pandemic Covid-19 is also visualized as the product of such technological innovations as per some of the scholars and scientists) by virtue of which the entire planet is trapped and powerless.

On the other end, the gigantic challenges of poverty, climatic changes, sustainability issues and so on, need grand dialogue and involvement of all stakeholders as well as the framing of some values and principles to better understand these challenges, risks and uncertainties involved (Blok, 2014; Blok et al., 2019). Upsettingly, some scientists believe that some vital verges have already been reached and that the earth's life-sustaining infrastructure is in danger. Taking into consideration these threats, there are immediate demands for sustained measures to shrink the associated effect on world security, health, and development. (Scherer & Voegtlin, 2020).

The United Nations, the European Union, multinational organizations and individual countries are searching for solutions to address these gigantic challenges. Many initiatives have been taken aiming to involve businesses as active partners and to promote cooperation between organizations and public and civil society players to facilitate sustainable growth. Accordingly, industries are now considered to be part of such societal issues and are demanded to look for the solutions to these societal challenges being socially responsible organization (Lubberink et al., 2017). Several moves were also initiated in Europe and United States for instance technological assessment organizations (TA), Technological Assessment and Ethical, Legal, and Social Aspects of emerging sciences (ELSA), the U.S Office of Technology Assessment (OTA), Netherlands Organization for Technology Assessment (NOTA). The purpose of these moves was to bridge the distance between society and technological innovations. However, the terminology of "responsible research" was first introduced in sixth framework programme (2002), aiming at fostering of developing relationship between ethics and technology throughout the world. Later on the terminology of "Responsible research and innovation" (RRI) was introduced in 7th framework programme, (2013) in Europe to develop trust of society on scientific inventions. (''Regulation (EU) No 1291/2013'' 2013) And now RRI is considered as much broader than these movements since it includes both societal and governance applications (Brand & Blok, 2019; Burget et al., 2017; Chatfield et al., 2017).

Responsible research & innovation (RRI) has emerged as one of the most crucial and paramount area of research which received little attention in scientific empirical researches. (Piccarozzi et al., 2018; Muller et al., 2018) Yet, the responsible innovation has got sudden increased popularity and momentum; even after the severe crises, the Europeans consider that the way towards sustainable, smart growth can be only through innovation where RRI would develop framework and policy for such innovation (Burget et al., 2017). So RI would be used as pulling strategy for Europe out of this economic crisis.

In other words, innovation with responsibility "responsible innovation" can be possible solution to all such threats and sustainability issues. Specially, during such period of world's drastic shift to new era of industrial revolution, the world needs to frame some principles and ethical/psychological bindings that should not only be able to manage this disastrous situation instead ensures the business organizations regarding their profitability, higher market and financial performances.

Responsible innovation (RI) presents a deliberate mechanism of stakeholder engagement as central governance mechanism considering them as shared & collectively responsible for the upcoming innovative products (Dreyer et al., 2017; Lubberink et al., 2017; Blok et al., 2015). It involves the use of firm's resources and capabilities to become firm's distinctive competency. Responsible innovation while becoming distinctive competency of the firm may lead the organization to gain competitive advantage and higher firm performance.

The major aim here is to divert the focus towards input side i.e. within the innovation process, through the inculcation of all relevant concerns regarding social, ethical issues of the

innovation by virtue of which that innovation may affect the health, safety, security, environment, privacy and other related values. Brand & Blok, (2019) In addition that governance mechanism would also guarantee a self & socially responsible/desirable, ethical and morally controlled product innovations. Whereas, this mechanism also caters the needs of business community while ensuring reasonable profits, since businesses are meant for profits. However, there are lack of evidences which suggest the way to put responsible innovation into practice and little is known regarding its applicability for economic benefits and gains. (Lees & Lees, 2018; Blok et al., 2015; Scholten & Van der Duin, 2015). Therefore, it is of utmost importance that empirical researches be carried out to put RI concept into practice and remove this tag of impractical approach.

CONCLUSION & LIMITATIONS

Highlighting the dark side of the industrial revolution 4.0 is again for the benefit of the world so as to prepare, plan, dedicate resources, strategize, implement and control the upcoming negative consequences caused by such radical revolution impacting every one's life.

We strongly believe that industrial revolution 4.0 may bring huge benefits, ease, flexibility, accuracy etc. along with betterment and up-gradation in the routine life of human however; the research presents serious concern over the sustainability of human race and considers the non-regulated, uncontrolled and irresponsible technological innovations as great danger. We believe that technological innovation can be used in two ways i.e. positive and negative whereby we should be careful about the negative and harmful consequences.

There are several limitations to our research since it was based on available information regarding IR 4.0 sought through various sources like research articles, reports, internet blogs etc. and all such are based on expectations and viewpoints since the information regarding IR 4.0 is still limited and ambiguous. Accordingly, our research is based on theoretical review and our opinions since its perspective article. Future researches may present empirical analysis of all the areas discussed in the article.

We would suggest to formulate a dedicated and holistic strategy covering all aspects of industrial revolution 4.0 especially considering the "Responsible Research and Innovation Framework" for all such issues and technical innovations. The formulated strategy should not focus on industrial point of view but should revolve around sustainability, wellbeing and welfare of the overall society. Further, legal framework is necessary to ensure the implementation of such strategy and human autonomy should be first priority in our mature societies. Most importantly, organizations should be made accountable for their products and it must be ensured that there should be contingency mechanism in artificially intelligent super machines like if they get out of control then there should be self-destruction mechanism.

There is strong need to devise ethical strategy to avoid the misuse of big data for personal benefits and earnings. Researchers and practitioners also need to work out on the enhancement of safety and security features cloud computing and big data stealing. It is advised to store data in multiple storages using the concept of distributed storages instead of single storage which is accessible with one password only. Further, scientific standards may be applied in case of use of Big Data. Although there are lot many challenges, however these can be addressed diligently and implementing technological solutions, norms and values, rules and procedures and legal framework.

REFERENCES

Alcácer, V., & Cruz-Machado, V. (2019). Scanning the industry 4.0: A literature review on technologies for manufacturing systems. Engineering Science and Technology, an International Journal, *22*(3), 899–919.

Abomhara, M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, *4*(1), 65-88.

Ali, B., & Awad, A. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors, *18*(3), 817.

Bartodziej, C.J. (2017). The Concept Industry 4.0 An Empirical Analysis of Technologies and Applications in Production Logistics. BestMasters. Springer Fachmedien Wiesbaden GmbH, 158.

Bean, R. (2016). Another Side Of Big Data: Big Data For Social Good.

Bihl, T. J., Young II, W.A., &Weckman, G.R. (2016). Defining, understanding, and addressing big data. International Journal of Business Analytics (IJBAN), *3*(2), 1-32.

Blok, V., Hoffmans, L., & Wubben, E.F.M. (2015). Stakeholder engagement for responsible innovation in the private sector: critical issues and management practices. Journal on Chain and Network Science, *15*(2), 147-164.

Brand, T., & Blok, V. (2019). Responsible innovation in business: A critical reflection on deliberative engagement as a central governance mechanism. Journal of Responsible Innovation, *6*(1), 4-24.

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': the US, EU, and UK approach. Science and engineering ethics, *24*(2), 505-528.

Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on Services Computing, *9*(1), 138-151.

Chatfield, K., Borsella, E., Mantovani, E., Porcari, A., & Stahl, B. (2017). An investigation into risk perception in the ICT industry as a core component of responsible research and innovation. Sustainability, *9*(8), 1424.

Chikhaoui, E., Sarabdeen, J., & Parveen, R. (2017)." Privacy and Security Issues in the Use of Clouds in e-Health in the Kingdom of Saudi Arabia ", Communications of the IBIMA, *2017*, 18.

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In 2012 International Conference on Computer Science and Electronics Engineering. IEEE, *1*, 647-651.

De Sousa Jabbour, A.B.L., Jabbour, C.J.C., Foropon, C., & Godinho Filho, M. (2018). When titans meet–Can industry 4.0 revolutionize the environmentally-sustainable manufacturing wave? The role of critical success factors. Technological Forecasting and Social Change, *132*, 18-25.

Dombrowski, U., & Wagner, T. (2014). Mental strain as field of action in the 4th industrial revolution. Procedia Cirp, *17*, 100-105.

Dreyer, M., Chefneux, L., Goldberg, A., von Heimburg, J. Patrignani, N., Schofield, M., & Shilling, C. (2017). Responsible Innovation. A Complementary View from Industry with Proposals for Bridging Different Perspectives, *9*(10), 1719.

Ekudden, E. (2018). Five technology trends augmenting the connected Society. Ericsson Technology Review, September 10, 2018.

Esposito, C., Castiglione, A., Martini, B., & Choo, K.K.R. (2016). Cloud manufacturing: security, privacy, and forensic concerns. IEEE Cloud Computing, *3*(4), 16-22.

Frey, C.B., & Osborne, M.A. (2017). The future of employment: How susceptible are jobs to computerisation? Technological Forecasting and Social Change, *114*, 254-280.

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, *35*(2), 137–144.

Helbing, D. (2019). Societal, economic, ethical and legal challenges of the digital revolution: from big data to deep learning, artificial intelligence, and manipulative technologies. In Towards Digital Enlightenment, 47-72.

Helbing D., Frey B.S., Gigerenzer G., Hafen E., Hagner M., Hofstetter Y., Hoven J.V.D., Zicari R.V., & Zwitter, A. (2019). Will democracy survive big data and artificial intelligence?. InTowards Digital Enlightenment, 73-98.

Horvath, D., & Szabó, R. Z. (2019). Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities?. Technological Forecasting and Social Change, *146*, 119-132.

Jazdi, N. (2014). Cyber physical systems in the context of Industry 4.0. In 2014 IEEE international conference on automation, quality and testing, robotics , 1-4.

Kagermann, H., Helbig, J., Hellinger, A., &Wahlster, W. (2013). Recommendations for implementing the strategic initiative industrie 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group. Forschungsunion.

Kaufman, L.M. (2009). Data security in the world of cloud computing. IEEE Security & Privacy, *7*(4), 61-64.

Kiel, D. (2017). What do we know about "Industry 4.0" so far. Proceedings of the International Association for Management of Technology (IAMOT 2017), 866-887.

Kiel, D., Müller, J.M., Arnold, C., & Voigt, K.I. (2017). Sustainable industrial value creation: Benefits and challenges of industry 4.0. International Journal of Innovation Management, *21*(08), 1740015.

Kwon, O., Lee, N., & Shin, B. (2014). Data quality management, data usage experience and acquisition intention of big data analytics. International Journal of Information Management, *34*(3), 387–394.

Lasi, H., Fettke, P., Kemper, H.G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. Business & information systems engineering, *6*(4), 239-242.

Lees, N., & Lees, I. (2018). Competitive advantage through responsible innovation in the New Zealand sheep dairy industry. International Food and Agribusiness Management Review, *21*(4), 505-524.

Liu, Y., Wang, L., & Wang, X.V. (2018). Cloud manufacturing: latest advancements and future trends. Procedia Manufacturing, *25*, 62-73.

Liao, Y., Deschamps, F., Loures, E.D.F.R., & Ramos, L.F.P. (2017). Past, present and future of Industry 4.0-a systematic literature review and research agenda proposal. International journal of production research, *55*(12), 3609-3629.

Lubberink, R., Blok, V., Van Ophem, J., & Omta, O. (2017). Lessons for responsible innovation in the business context: A systematic literature review of responsible, social and sustainable innovation practices. Sustainability, *9*(5), 721.

Martin (2017). Industry 4.0: Definition, Design Principles, Challenges, and the Future of Employment.

Müller, J.M., Kiel, D., & Voigt, K.I. (2018). What drives the implementation of Industry 4.0? The role of opportunities and challenges in the context of sustainability. Sustainability, *10*(1), 247.

Müller, J.M., Buliga, O., & Voigt, K.I. (2018). Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0. Technological Forecasting and Social Change, *132*, 2-17.

Piccarozzi, M., Aquilani, B., & Gatti, C. (2018). Industry 4.0 in Management Studies: A Systematic Literature Review. Sustainability, *10*, 3821.

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100 million dollar data breach. Journal of Information Technology Teaching Cases, *8*(1), 9-23.

Roblek, V., Meško, M., & Krapež, A. (2016). A Complex View of Industry 4.0 . SAGE Open April-June 2016: 1–11.

Rodrigues, J.J., Compte, S.S., & De la Torre Diez, I. (2016). Cloud computing on e-health. e-Health Systems: Theory and Technical Applications, 191-207.

Russell, S.J., &Norvig, P. (2016). Artificial intelligence: a modern approach. Malaysia; Pearson Education Limited.

Scherer, A.G., & Voegtlin, C. (2020). Corporate governance for responsible innovation: Approaches to corporate governance and their implications for sustainable development. Academy of Management Perspectives, *34*(2), 182-208.

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, *10*(7).

Sung, T.K. (2018). Industry 4.0: a Korea perspective. Technological forecasting and social change, *132*, 40-45.

Scholten, V. E., & Van der Duin, P. A. (2015). Responsible innovation among academic spin-offs: how responsible practices help developing absorptive capacity. Journal on Chain and Network Science, *15*(2), 165-179.

Takabi, H., Joshi, J.B., & Ahn, G.J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, *8*(6), 24-31.

Wang, L and Wang, G. (2016). Big Data in Cyber-Physical Systems, Digital Manufacturing and Industry 4.0. I.J. Engineering and Manufacturing, *4*, 1-8.

Wang, Y., Kung, L., & Byrd, T.A. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. Technological Forecasting and Social Change, *126*, 3–13.

Winfield A.F., & Jirotka, M. (2018). Ethical governance is essential to building trust in robotics and artificial intelligence systems. Phil. Trans. R. Soc. A, 376 (2133).

Zhong, R.Y., Xu, X., Klotz, E., & Newman, S.T. (2017). Intelligent manufacturing in the context of industry 4.0: A review. Engineering, *3*(5), 616-630.