The Fourth Industrial Revolution

Industrial revolution is a crucial improvement and changes in the history of humanity of our current modern world. An Industrial Revolution at its core occurs when a society shifts from using tools to make products to using new sources of energy, such as coal, to power machines in factories. The first industrial revolution was started in the late 18th century, in Britian when steam machine was invented helped to boost up the manufacturing speed. After two and half centuries later, we had experienced the second and third industrial revolution, and now we are stepping into the era of fourth industrial revolution.

The fourth industrial revolution optimises the computerisation of the current industry 3.0. Thanks to the addition of 5G technology, computers able to connect and communicate with one and other to ultimately make decisions without human involvement. A combination of cyber-physical system, the Internet of Things and the Internet of Systems make Industry 4.0 possible and the smart factory a reality. As a result of the support of smart machines that keep getting smarter as they get access to more data, our factories will become more efficient and productive and less wasteful. Ultimately, it's the network of these machines that are digitally connected with one another and create and share information that results in the true power of Industry 4.0.

The first steps of the new industry revolution 4.0 were cloud technology, the improvement of the ability to collect data and analyse Big Data. The Big Data concept is a set of technologies that are used to handle large amount of data compared to “standard” scenarios, ability to work with fast coming data in very large volumes, and able to work with structured and poorly structured data in parallel in different aspects.[1] An example of Big Data can be the Large Hadron Collider, which produces a large amount of data and does it all the time. The installation continuously produces large amounts of data, and scientists with their help solve many problems in a short time.[2]

However, there are some risks and challenges should be included while deploying cloud technology and big data. The biggest challenge that should be considered is the security of the big data cloud environment. One of the most significant Big Data security vulnerability is the leakage of Big Data, tentatively defined as disclosures of Big Data assets.[3] In the case of Big Data Leaks, however, one may want to blame the effect of redundancy, a phenomenon well known to social scientists. In traffic pattern analysis, for instance, trip redundancy - making unnecessary multiple trips to the same destination, e.g., facilitated by low fuel costs - is well known to be a traffic multiplier, and therefore a non-linear risk booster, as increasing traffic increases the probability of accidents more than proportionally. Due to trip redundancy, even a small decrease in transportation costs can translate into a large traffic increase, and consequently in a substantial increase of accidents. [3]

Therefore, to encounter the problem of “Big Data Leaks”, although the systematic study of Big Data Security is still immature but however there are still some practices are best to work on top-level cybersecurity. These functions are Know, Prevent, Detect, Respond and Recover. Know is to know the level of the replication and distribution of the data in the Big Data storage. Prevent is to make sure security protection the same across all the Big Data storage system, avoid early provisioning of unnecessary data, anonymising then analyse and avoid violations to data usage

regulations during the computation of analytics. [3]

The other key component for new industry revolution 4.0 is the Internet of Things (IoT). The Internet of Things is a computing concept that describes all physical objects will be connected to the Internet and be able to identify themselves to other devices. The Internet of Things ecosystem consists of smart objects, intelligent devices, infrastructures, transportation factories and machines. Industry revolution 4.0 refers to the use of automation and data exchange in manufacturing. Industry revolution 4.0 uses an Internet of Things, or at least an Intranet of Things, in order to perform digital manufacturing. All devices, robots, simulations, and tools have sensors and provide data.[4]

The security aspect is the biggest challenge faced by the Internet of Things connected devices. The IoT application data can be personal, enterprise, industrial or consumer but stored data should be secured against theft, tampering & protected in the transit and at rest. For example, an IoT application may stores currents and historical data of machineries, individual's health, shopping behaviour, location, finances and quantity of inventory, business orders etc. Security is a take in account when transmitting data across the Internet or through secured private network. [4]

The Government regulations such as Health Insurance Portability and Accountability(HIPA) Act or restrictions on transporting data across international borders can be applied as safety precautions. The Federal Trade Commission (FTC) report on the IoT highlights some of the risks & suggest some ways to overcome them. For example, MyQ Garage system device from Chamberlain allows a user to open and close garage door from a Smartphone. But Veracode found that a potential burglar could gain access to the device and use it to find open or closed state of garage door and find opportunity to rob the house. The key IoT security tasks should ensure that proper application level protections like Distributed Denial of Service (DDoS) attack mitigation are in place. It should also incorporate measures to confirm the identity of entities requesting access to any data including multi - factor authentication. [4]

Cyber physical system is one of the most significant key factors and a fundamental enabler for industry revolution 4.0. Cyber-Physical systems (CPSs) represent the technological asset of the fourth industrial revolution. Such systems, integrating a physical and a cyber domain, provide a pervasive and collaborative industrial infrastructure able to support the digital representation of data/information along the product and process lifecycles. The growing demand of autonomy and the need to reduce both the time in taking decisions and the transmission bandwidth are pushing designers in integrating Cyber physical system with intelligent mechanisms[5]. The cyber physical system utilization in industrial settings is provisioned to revolutionise the way enterprises conduct their business from a holistic viewpoint[6].

One of the major challenges faced by the cyber physical system is still security. Security, in contrast, is traditionally viewed as a data or communications security problem to be taken care by computer scientists and/or computer engineers. However, cyber physical systems have additional characteristics that provide chance to attackers; for example, their real-time behaviour means that attackers can cause havoc without stealing or corrupting data, by simply altering the timing of key computations is enough to put the system into an unsafe state. cyber physical systems are also sensitive to a wider range of attacks and design flaws than are information technology (IT) systems. A complete threat model needs both the environment, including the attacker, and the system under threat. Any threat, whether from an attacker or from a bug, can

use the security vulnerability of a failure of the system to fully go along with a specification of its characteristics, whether indirect or direct. Disturbing the timing of real-time operations can result in the physical plant to fail[7].

New methodologies, architectures, and algorithms are required to make sure that cyber physical systems meet their required safeness levels. Security techniques must be applied at both design time and runtime. System design provides several opportunities to upgrade the safety and security levels. Designers can examine system models to determine attack surfaces and safety issues and to identify the effectiveness of our solutions to these problems. Synthesis of implementations of cyber physical systems can be used to make sure that specifications and architectures are correctly translated, preventing the introduction of faults that can compromise safety or security. At runtime, we can monitor and analyse system properties to determine attacks and bugs at an early stage. Designs can perform runtime monitors to analyse both the cyber and physical behaviours of the system, comparing observed behaviour with predictions. System components can be fingerprinted to make sure the configuration and consistency with system requirements are always correct[7].

In conclusion, although the era of fourth Industrial revolution has getting closer and closer to our current modern world. However, there are still have many challenges must be faced by the researcher and scientists and to be solve by them in order to prevent the integrated system that leads by the Cloud technologies, cyber physical system, Internet of things systems and etc collapse. Let us look forward to the positive consequences brought by the new industry revolution to the world economy, to the society and to our live. We believe that when the day comes, the advantage will be for companies owning a unique platform that unites many people in around the world.