International Journal of Internet of Things 2020, 9(1): 1-11
DOI: 10.5923/j.ijit.20200901.01

Industrial Internet of Things Common Concepts, Prospects and Software Requirements

Joseph Kalunga[1,*], Simon Tembo[1], Jackson Phiri[2]

[1]Electrical and Electronics Department, School of Engineering, UNZA, Lusaka, Zambia
[2]Computer Science Departments, School of Natural Science, UNZA, Lusaka, Zambia

Abstract The manufacturing and many other critical Infrastructures industries are posed to introduce the initiative popularly known as Industry 4.0 or industrial Internet of things. In developed nations, Industry Internet of thing technologies have already been implemented in varieties of industries like health care, logistics, avionics, waste management, military, smart cities and many other fields. So far, the initiative has provided various benefits that include improved efficiency, productivity and cost reduction. However, the prospective transformation of Internet of things Technology would see some change in the way companies approach manufacturing and other industries in terms of in-house software development, security design and implementation. Considering the fact that Industry 4.0 belong to the family of critical infrastructures, ICT application development, security design and implementation will always be complex, costly, large in scope, involves heterogonous network of things that encompasses dealing with a diverse set of Technological components. This complexity may result in misconfiguration, misappropriation and misconception of facts on part of users, software developer and security architects. For this reason, this paper details information technology component of Industry 4.0 framework with an objective to amplify and clear misunderstanding of key terminologies and the basic composition of industry 4.0 framework. The study also highlights industrial Internet of things prospects and barriers and articulates effective requirement elicitation process for application customization, development, and technological fusion and Security solutions implementation. The methodology of this paper is based on two research techniques namely literature review and a study on application scenarios from research communities and industries. Because of these, simple and effective model for requirement engineering is proposed.

Keywords Internet of things, Industry 4.0, Industrial Internet of things, Cyber Physical Systems, Critical Infrastructure, Industrial Evolution, Requirement Engineering

1. Introduction

Internet of things (IoT) technology is rapidly growing, raising severe positive prospects and negative concern to users, software development team, organisations, industries, governments and research community. IoT involves the networking of every physical object that contains embedded technology to communicate and sense or interact with their internal states or the external environment [1]. IoT technologies are already in use in varieties of industries like health care, logistics, avionics, waste management, military, smart cities and many other fields in auspice of industry 4.0 initiatives.

Statistics have indicated that about 26.6 billion IoT devices were activated in 2019 sharing global market as Smart Cities (28.6%), Industrial IoT (26.4%), Heath Care (22.0%), Smart homes (15.4%) and automobile (7.7%) [2]. Researchers have also projected over 75 billion IoT device activation by the year 2025 and with the year 2020 upsurge of about 40% towards Industrial IoT specifically health care industry [3].

Kemps and Bera's [2] projected rise in industrial Internet of thing market share may act as a focal point for the future Industrial IoT Research and Development (R&E). The manufacturing industry and many other critical Infrastructures industries are posed to introduce the initiative popularly known as fourth Industrial Revolution or Industry 4.0. In industry 4.0 the real and virtual world is impeccably connected giving rise to what is referred to as Cyber-Physical Production Systems [4]. As the result, traditional manufacturing processes will witness an enormous transformation which will change the way companies approach manufacturing and critical infrastructure industries [5]. These changes will also affect software development and security implementation. There will always be new organisation demands for software customisation, upgrading, fusion and development of new

* Corresponding author:
josephkalunga@yahoo.com (Joseph Kalunga)
Published online at http://journal.sapub.org/ijit

application, software or security solutions. However, the complexity and diversity nature of Industry 4.0 framework makes System Requirement elicitation process difficult. Effective requirement elicitation may call for full contextual understanding of the industry, key technological components and their technical working relationships.

This paper details information technology component of Industry 4.0 framework with an objective to amplify an understanding on the basic configuration of industry 4.0. The study also highlights industrial Internet of things prospects and barriers and articulates effective requirement elicitation process for application customisation, development, and technological fusion and Security solutions implementation.

2. Scope and Methodology

This paper is structured as follows: (1) Start with contribution of the study (2) then Related works, (3) Industrial Evolution (4) industry 4.0 prospects and barriers, (5) Proposed effective requirement Engineering Model, (6) and finally conclusion.

The methodology of this paper is based on two research techniques namely literature review and the study on application scenarios from research community and industry. When conducting literature review, relevant papers were identified through title, abstracts, and keywords from interdisciplinary journals or repositories. Additionally, tables were employed extensively to present, summarise, organise, contrast and compare relevant tasks. When analysing key industry IoT components, the hierarchical Input/Out (HIPO) chart was employed. HIPO chart provide a modular approach to system analysis and hence suitable for complex system analysis and requirement Modelling [6].

3. Contribution of the Study

The study contributes the following:

- Amplifies an understudying between IoT, IIoT, CPS and Industry 4.0.
- Highlight the philosophy behind Industry 4.0 frameworks.
- Identify critical Information Technology components of Industry 4.0.
- Proposed component and functional based requirement engineering model for industry 4.0.

4. Related Works

In this section, the study seeks to clarify the misconception surrounding the terms Internet of things (IoT), Cyber-Physical Systems (CPS), Industrial Internet of things (IIoT), industrial 4.0 and critical infrastructure. It also offer a brief understanding of IoT in general, history of industrialisation with the special focus on industry 4.0 and its philosophy, components and general characteristics. The paper also discusses the integration of IoT in to industrial 4.0. The integration of IoT in to manufacturing industry results in communication hub called "IIoT infrastructure" from elementary perspectives. Figure 1 summarises common attributes between IoT, IIoT and Industry 4.0.

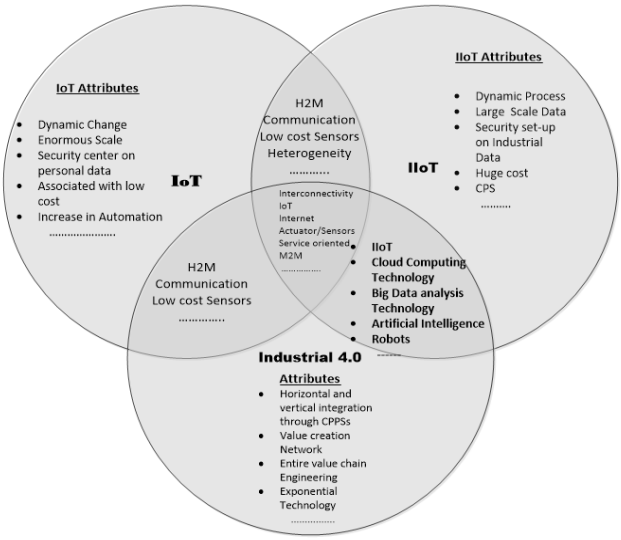

Figure 1. IoT, IIoT, Industry 4.0 attributes and the common concepts

4.1. Internet of Things

There is no official definition of internet of thing (IoT) [7]. However, researchers have been defining it in differently ways depending on its perspective [8]. For example, the term IoT may refer to the network of physical objects, devices, instruments, vehicles, buildings and other items embedded with electronics, circuits,software, sensors and network connectivity that enables these objects to collect and exchange data [9]. Subha [10] also defined Internet of Things (IoT) as dynamic global information network consisting of Internet-connected objects, such as Radio frequency identifications (RFID), sensors, actuators, as well as other instruments and smart appliances that are becoming an integral component for the future Internet.

4.2. Cyber Physical System

In industrial IoT perspective, Internet of things could be defined as a cyber-physical system that integrates billions of heterogeneous devices and smart technology [11]. Cyber-physical system (CPS) is a brain behind industrial Internet of Things philosophy. CPS provides a mechanism that is controlled and monitored by computer-based algorithms, tightly integrated with the Internet, services and its users. In CPS, physical, virtual and software components are deeply tangled, each operating on different dimension and scale, exhibiting multiple and distinct behavioural modalities, and interacting with each other in a lot of ways that are dynamic with context. In summary, CPS are at the centre of industrial 4.0, IIoT and similar to IoT in general because they share the

same basic architecture, although CPS presents a higher combination and coordination between, virtual, physical and computational elements [12]. The other similarity and misconception may exist between IoT and IIoT.

4.3. Internet of Things and Industrial Internet of Things

The different between Internet of thing and Industrial Internet is lean because the two concepts shares many technologies include cloud computing, sensors, actuators, connectivity, data analytics and many others. The other similarities are in intrinsic characteristics. Both IoT and IIoT poses similar attributes include Machine-to-Machine (M2M), Machine-to-Human (M2H), communication, dynamic, heterogeneity, Service Oriented and many other characteristics illustrated in figure 1. However, the different between the two lays in context of application, ownership, equipment durability, cost and levels of security concerns and scale of application.

For an example, IoT applications connect devices across multiple verticals at a moderate scale in field of agriculture, healthcare, enterprise, consumer and utilities, as well as government and cities [13]. IoT devices include smart home appliances, smart phones, smart wearable (smart watches), fitness bands and other applications that generally do not create emergency situations if something goes wrong. These smart devices are normally cheaper and are installed for personal reasons [11].

On the other hand, IIoT applications connect machines, people, processes, Cyber-Physical Systems and sensors, smart devices in the fields stated above in addition to oil and gas manufacturing industries at large scale. IIoT devices are normally durable in nature, Proprietary and cost bit higher as compared to IoT devices. System failures and downtime in IIoT deployments can result in high-risk situations or even life-threatening situations [14]. IIoT applications are also more concerned with improving efficiency and improving health or safety, versus the user-centric nature of IoT applications. Initially, when the concept of IIoT conceived, it was coined to improve efficiency and productivity in manufacturing industries, but currently smart concept is gaining ground in many fields especially, environment, military, healthy, avionics and many other fields. In future, we shall see IIoT at center of human survival and at most influence human existence. The other resemblance and fallacy exists between IIoT and Industry 4.0.

4.4. IIoT and Industry 4.0

There are so many researchers published articles on Internet of thing, Industrial internet of things and industrial 4.0, however the meaning and relationship between the three concepts still remains quiet blurry. Just like IoT concept, there is no universal acceptable definition of Industrial Internet of Things and industrial 4.0. The definition and the relationship among the two concepts depend on the context of an application [15]. Industrial Internet of Things refers to the interconnected sensors, actuators, instruments, machines and other devices connected together with computers to support manufacturing industry or utility industry [16]. This connectivity allows data collection, exchange, and analysis, potentially facilitating improvements in productivity and efficiency as well as other economic benefits. This concept is also true for the relationship IoT and Industrial 4.0. Additionally, IIoT is based on the development of the distributed control system (DCS) that permits higher degree of automation by using cloud computing, big data analysis, artificial intelligence and robotics to refine and optimize the process controls [16]. In other words, IIoT is the backbone under which industrial 4.0 is underpinned. It provides enabling technologies that connect device, machines, people, big data analysis, predictive maintenance and many other enabling technologies. On the other hand, Industry 4.0 has a touch of government and corporate initiative [5]. Strategically, industry 4.0 philosophy is based on digitalisation, creation of new technologies; learn new initiatives, automation and efficient use of materials. Having stated that, Industrial 4.0 could be defined as:

- "Focuses on the end-to-end digitisation of all physical assets and processes as well as integration into digital ecosystems with value chain partners" [17].
- "The era of automation, of the digitalized factory and digitalized products – the fourth phase of industrial revolution" [18].
- "The Collective term for technologies and concepts of value chain organisation. Within the modular structured Smart Factories of Industrie 4.0, CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. Over the IoT, CPS communicates and cooperates with each other and humans in real time. Via the IoS [Internet of Services], both internal and cross- organizational services are offered and utilised by participants of the value chain" [19].

In this study, we defines industrial 4.0 as "Evolution towards industrial automation and data exchange of every object which include people, materials, cyber-physical systems (CPS), The internet of things (IoT), big data analysis, cloud computing, cognitive computing, artificial intelligence and many other technologies depending on the context of an application".

From our definition, we assume that, IIoT is the subset of fourth industrial revolution, thus encompasses areas which are not normally classified as industries, such as smart cities, smart utility and smart public installations include military and national security installations which are normally referred to as critical infrastructure. The combination of industry 4.0 and IIoT yield globally competitive positive results that include transparent, flexibility, efficiency and zero downtime which are the most needed requirements in modern industries. Even though, IIoT and industry 4.0 co-exists, there are some differences between them in operation and application. Sontag [20], highlighted some differences between the two concepts as summarised in table

1.

Table 1. Difference between IIoT and Industry 4.0

IIoT	Industry 4.0
Applied to all sectors where industrial / professional equipment is used	Focuses primarily on the manufacturing sector
Connect Assets and Data Management	Digitization of the complete value chain.
Private Sector Driven	Associated with Governmental and Institutional initiatives
Concentrate on ICT Components fusion	Complete value chain digitalization
Subset of Industry 4.0	IIoT plus all manufacturing Assets
Source of Privacy & data Security	IIoT inject Privacy & Data Security issues

Table 1 highlights the differences between Industrial Internet of thing and industry 4.0. As indicated already, IIoT is a synonym to industry 4.0. The difference lays in context of application and operation. Other major difference is that, IIoT is more specific to computing and sharing of information among industrial components through internet technologies while Industry 4.0 is the broad term encompasses the entire digital change of the industry or manufacturing entity.

4.5. Critical Infrastructure

According to [21] IoT, CPS, IIoT and industry 4.0 represent life of critical infrastructure (CI) which conveys interconnection of heterogeneous devices in different application perspectives. Today, CIs just like IoT family have become an integral part of cyberspace and they play a vital role in supporting many of our daily activities (including travel, water and power usage, financial transactions, telecommunications, and so on) [22]. Alcaraz & Zeadally further stressed that, reliability, high-performance; continuous operation, safety, maintenance and protection of these CI are national priorities for many countries around the world. CI may include assets and their supportive heterogeneous devices, networks either physical or virtual, underpinning the functioning of an economy and society [23]. Most often, CI determines the security, prosperity, wellbeing and resilient of an entire nation and thus is always on the government protective agenda [24]. Modern CIs are connected to the internet and may contain heterogeneous devices that can sense data and transmit it to remote agent or location. In future internet, Critical infrastructure will be referred to as intelligent processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of people and the effective functioning of government [23]. A Critical Infrastructure is evolutionary and ambiguous just like CPS, IIoT and industry 4.0 in nature [24]. Examples of CI may include roadways, bridges, military bases and airport, mass transportation systems, waste treatment plants, energy facilities, hospitals, public buildings or communication facilities and may act as the driver to national economy. CIs just like IIoT are very important nation entities and thus should be highly protected [22].

5. Industrial Evolution

Industrial revolution began in 18th century through the use of water and steam power to drive mechanical engines [25]. Steam engine was employed to mechanise production and improve productivity. Steam engine level of industrialisation is sometimes referred to as industrial 1.0 [19]. According to Jeevitha and Ramya [26], industrial 1.0 resulted in reduced manual labour force, increased productivity and grew businesses.

The industrial 2.0 generation began in 19th century through the discovery of electricity and assembly line production. Second industrial evolution principles were adopted in automobile production, agriculture sector and steal production [26]. It drastically changed production processes resulting in faster steal production, building of railways, automobile and cost reduction. This period inherited all the attributes of first industrial evolution and saw the development of a number of management programs that made it possible to increase the efficiency and effectiveness of manufacturing facilities [26].

In third generation, computers were introduced in production line to control the industrial processes. Industrial 3.0 started in 1970s with an introduction programmable control systems, computer memory and extensive use of robots [18]. It improved efficiency, reduced human error, improved quality of the product as compared to industrial 2.0 and industrial 1.0. However, industrial 3.0 opened a new challenge to industry involve cyber security and data privacy [19].

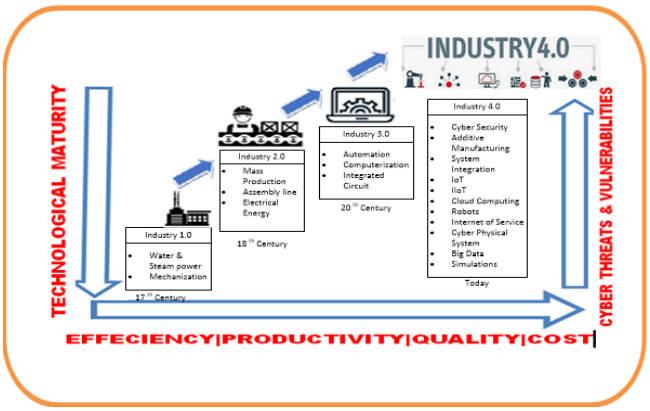

Figure 2. Industrial Evolution

Currently, we are implementing industrial 4.0. The Current industrial IoT trends and initiatives are aimed at connecting almost everything. It has two types of connections internal network and internet connections that eventually form single network. Industrial IoT connects equipment, machines and devices in industries such as

transportation, power generation, and oil and gas, and is set apart from other IoT applications by its daily effects on human safety. Industrial 4.0 combine many other technologies in addition to those found in third generation include computer networking, automation, IoT, cloud computing, robots, artificial intelligence, big data analysis and other technologies underlined in figure 2.

5.1. Birth of Industry 4.0

The term industrial 4.0 was initiated in 2011 by a group of German business associates, academician and political representatives to craft an initiative aimed at improving the manufacturing industry's competitiveness [27]. The basis for the fourth industrial revolution is availability of all relevant information in real time by connecting all instances involved in the value chain [26]. This initiative is rapidly growing in different place particularly United States, Japan, China, the Nordic countries, and the United Kingdom. According to German high-tech 2020 strategy, industrial 4.0 is seen as a key to economic growth, employment creation, prosperity and modality to improve quality of life. The strategy further stressed essential industrial components to support decision making, efficiency, productivity, quality of product and minimise production costs. These benefits could be achieved through automation and data exchange of various smart manufacturing technologies such as Cyber Physical Systems, Internet of things, Internet of service, cloud computing artificial intelligence and many other technologies [5]. According to [28] industrial 4,0 is therefore referred to as smart industry and encompasses technological evolution from embedded systems to cyber-physical systems (CPS). In short, Industry 4.0 emanates throughout the automation, Internet of Things, Data and Service path [28]. Through the evolution of the Internet, the real world and the virtual world are increasingly converging, to form an "Internet of things" or "Industrial Internet of things" [29]. Essentially Industry 4.0 movement is envisioned to bring together humans, robots and automation in ways never before possible. This consequently will result in creation of smart factories. In smart factories, cyber physical machines monitor the processes in the assembly line and make decentralised decisions [30]. Smart factories through Internet of Things (IoT) technology will communicate and cooperate with both machines and humans in real time via the web. The implication is that smart cities may inherit both benefits and down side of IoT technologies.

5.2. Industrial 4.0 Philosophy

The philosophy of Industrial 4.0 or production 4.0 or IIoT concepts are mainly used in Europe. As mentioned earlier, it has the root in German. However, similar initiatives were started in many countries. In United States Industrial 4.0 is referred to as Industrial Internet Consortium (IIC) [18]. The industrial internet consortium was founded by companies like AT & T, CISCO, General Electric, IBM and Intel [31]. The essence of this Consortium is to promote new Internet technologies not only in manufacturing industries but also in many other sectors. Furthermore, these creativities are in Japan under the name Industrial Value-Chain Initiative (IVI) [27]. Just like US Initiators are major Japanese companies [32]. India and Malaysia also took initiatives similar to the German political initiative "Industry 4.0" [4]. These initiatives are intended to play a decisive role in the shift nation from low-wage countries to global industrial through the power of IoT. South Korea also has invested heavily in so-called smart factories [33]. In several European countries there are other activities comparable to the German political initiative "Industry 4.0", such as France du „Industrie du futur" in France [28]. Made in china 2015 plan is also another plan drew inspiration from German industrial 4.0 plan. But china plan is broader in scope because its manufacturing guiding principles are innovative-driven, emphasize on quality over quantity, optimise the structure of Chinese industry, and nature talent [31].

6. Components of Industry 4.0

Although "Industry 4.0" is the common term referring to the fourth industrial revolution, academics still struggle to properly define the approach [17]. This makes it even harder to distinguish the main components of such an approach. According to Hermann, Pentek, and Otto [34], the generic industry 4.0 framework contains four main IT components include Cyber-Physical Systems, IoT, Cloud Computing and cognitive computing. These four components have other constituents as depicted in figure 3.

6.1. Cyber Physical Systems

As mentioned above, Cyber- physical system (CPS) is a brain behind industry 4.0 philosophy. CPS provides a mechanism that is controlled and monitored by computer-based algorithms, tightly integrated with the Internet, services and its users. The aim of cyber-physical system is to integrate computation units in to physical processes of industry 4.0. This means that computers and networks are able to monitor the physical process of manufacturing entity at every stage. CPS consist instruments for social machine, augmented operator and virtual production. The development of such a system consists of three phases include identification, integration of sensors and actuator and the development of sensors and actuators [19].

6.2. Internet of Things

Internet of Things platform may include subcomponents such as mobile devices, IoT application, interfaces, big data analysis, authentication & fraud detection, smart sensor and machine automation [35]. The Internet of Things enables objects, things, services and machines such as mobile phones and sensors to connect and communicate with each other as well as human beings to solve a specific production problem. The integration of such technology allows things/object to work and solve problems independently.

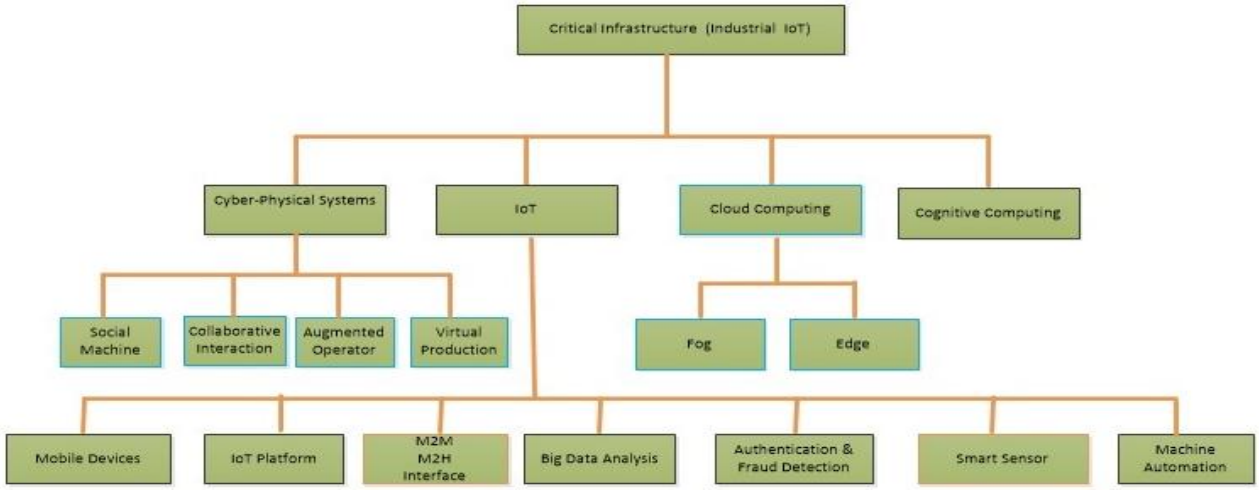

Figure 3. Generic Components of IIoT

6.3. Cloud Computing

Cloud Computing Technology is one of the major components of industry 4.0. Cloud computing has been in existence for a long time and it include a relative new system logic that provide a huge space of storage for industry 4.0 users. It is important to note that, the performance of cloud computing is kept on improving because of the huge benefits mostly focused on cost reduction. However, the functionality of the machine data, hardware and application/software will continue to be stored in the cloud storage systems as a service, allowing production system to be more data-driven. Thus, minimizes Industrial departments limitation since data sharing will occur across the sites for production-related undertaking. For this reason, cloud computing is becoming one of the most critical consideration for industrial companies system development process. However, there are downsides of heavily depending on cloud computing. For example, sending all the data collected all the time to cloud has high costs in terms of bandwidth, storage, latency, energy consumption (for communication) and so on [36]. To solve this problem fog and edge computing were employed in cloud computing infrastructure.

Cloud computing in industry 4.0 concept is supported by fog and edge computing. Fog computing provides the missing link for what data is needed to be pushed on the cloud, and what data can be analyzed locally, at the edge. Fog computing can create low-latency network connections between devices and analytics endpoints. Some computing could be done at the site or near the site where huge data is originated. Edge Computing provide a computing that's done at or near the source of the data, instead of relying on the cloud at one of a dozen data centers to process all the data. Edge computing is done to facilitate real time processing.

6.4. Cognitive Computing

Cognitive computing is another major component of industry 4.0. Cognitive computing provide techniques for solving complex problems that may have dynamically shifting situations and information rich data that tend to frequently change and sometimes conflicting with each other. Human being may deal with such a problem in a very slow manner by solving goals and objectives contrary to traditional computing algorithms which are not able to adapt to such changes. To solve this complex problem, cognitive computing is employed in industry 4.0 or IIoT. Cognitive computing just like many other Industry 4.0 or IIoT key terminologies has no industrial or academic agreed upon definition. However, cognitive computing refers to the technology that mimics the way human brain function and how it approaches complex problem solving. Cognitive computing is contextual, adaptive, and interactive and state oriented in nature. Cognitive computing industrial software and security design must support both parallel and distributed computing and are powered by underlying computing Infrastructure [36].

7. Prospective and Barriers

Several distinct prospects and barriers exist in the industry 4.0. Table 2 summarizes generic prospects and barrier to industry 4.0 implementation.

Table 2. Industry 4.0 Prospects and Barriers

Prospects	Barriers
+ Increased Data Accessibility	- Huge Implementation Cost
+ Market Serenities	- Complexities of Combining New Technology and Cyber Physical System
+ Open up New Employment and Service	- Security
+ Flexible operations	- Regulatory hurdles
+ Improved supply chain transparency	- Lack of Predefined IIoT Standards
+ Efficiency and Mass Production	- Relevant Skills and Expert suport Port Hurdles

7.1. Industry 4.0 Prospects

According to Sund [27], Industry 4.0 positive prospect may include increased data accessibility, market serenity, open up new employment, flexibility and improved supply chain transparency. Other are improved quality of service (QoS), efficiency and enhancement of productivity.

7.1.1. Increase Data Accessibility

By extracting the vast amount of manufacture data contained within a single setting or Production site, companies can use this information to make real time adjustments in order to improve both product quality and production efficiency. Increased data accessibility can help companies diversify revenue streams and expand revenue opportunities.

7.1.2. Market Serenities

Industry 4.0 can help change the existing market dynamics, through the introduction of new business models and strategies. By responding more flexibly to customer needs, companies can create new revenue streams and reduce time to market.

7.1.3. Open up New Employment and Service

There is an increase in cybercrimes targeting industry 4.0 infrastructures [37]. Companies still have a long way to go in strengthen their cyber defenses and there are significant opportunities for companies that can offer solutions to help other companies attain the full benefits of connected manufacturing in a manner that does not attract cyber criminality.

7.1.4. Flexible Operations

Companies can use combinations of big data and real time information applications to implement flexible pricing models, product improvement, enhances user centric production and promote new marketing strategies in real time.

7.1.5. Improved Supply Chain Transparency

Through improved monitoring capabilities industries and companies can further reorganize their supply chain and inventory control operations. Production System can even be made more efficient through introduction of Industry 4.0 related technologies.

7.1.6. Efficiency and Mass Production

Industrial automation can improve efficiency in terms of productive, quality of service and service delivery. Efficiency, improved quality of product and mass production are some of the goals behind industry 4.0 initiative.

7.2. Barriers to Implementation

7.2.1. Huge Cost

Setting up an industry 4.0 concept based business or company attracts huge capital injection in terms of machinery, human resource, infrastructure and technology. Additionally, industry 4.0 concept demand for huge operation cost, political and social support.

7.2.2. Complexities of Combining New Technology and Cyber Physical System

Industry 4.0 is the fusion of many technologies [4]. For this reason medium industries have limited possibilities to invest in state of the art equipment and will have to maneuvers in fragmented production environment, by merging both old and new equipment in production line. This could bring legacy equipment to the required standard through retrofitting of heterogeneous devices.

7.2.3. Security

Security and data privacy challenge as a potential to compromise key Industrial IoT (IIoT) safety services include availability, confidentiality and data integrity [38]. Other consequences of security and data privacy bleaches include, loss of lives, embarrassment and discontent in public domain that negatively affect the entire human life cycle be it political, social and economic.

7.2.4. Regulatory Hurdles

Industry 4.0 regulatory systems vary from country to country because of differences in philosophy, technological, social, political and economic market restriction. For example, in most Western markets, everything that is not explicitly forbidden is allowed. However, In Japan, it is often a requirement to obtain a permission in order to pursue activities within certain areas, significantly slowing the process down [27]. Other example is the recent United States and china trade regulatory conflict [39].

7.2.5. Lack of predefined IoT standards

The rapid growth of IoT in manufacturing sector may be a cause for significant concern. IoT Technology is not only overwhelmed with security, authentication and access control issues, it does not also work as it should in fourth industrial revolution because of the absence of acceptable standard [39]. The absence of effective regulation, standards and weak governance may result in continuous downward trend in implementation of industry 4.0 initiatives.

7.2.6. Relevant Skills and Expert support hurdles

In most nations if not all, there is an existence mismatch between job applicant’s qualification and skills requirements resulting from implementation of new technology. In the scenario where Industry 4.0 technologies will be widely adopted by 2020, the demand-supply gap will be widen even further unless necessary actions are taken by each country. Some countries have already taken relevant redressing steps. For instance, some governments of the BRICS nations have undertaken independent initiatives aimed at promote

vocational education and skill development in their countries. However, there are still significant efforts required focusing on the skill development of Industry 4.0 [39].

8. Prospective and Barriers

The prospective transformation of Internet of things Technology would see some change in the way companies approach manufacturing and other industries in terms of in-house software development, security design and implementation. Industry 4.0 being a critical infrastructure, application development, security design and implementation is complex, costly, large in scope, involves heterogonous network of things that encompasses dealing with a diverse set of Technological components. So far, researchers, organisations and operational bodies of standards have proposed several industry 4.0 system development and security implementation methodologies as highlighted in [40] and [22] respectively. However, models for requirement engineering of new industrial IoT application development, customization, application fusion or machine/device plugin have not been considered adequately. Even though, Security and software development implementation process is highly dependent on the clear requirement engineering model. Industry 4.0 requirements include the fusion of Internet of things, machines, computer and people, enabling intelligent using advanced data analytic for transforming business outcomes [40]. For that reason, industry 4.0 requirements specification is proven difficult. To simplify the process, component and function based requirement engineering model is proposed and detailed in figure 4.

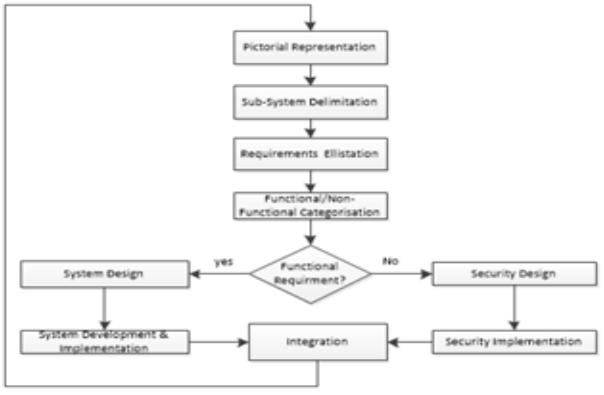

Figure 4. Proposed Model for Industry 4.0 Requirements Engineering

8.1. Pictorial Representation

In the new model, broad industry 4.0 system is represented in the rich picture. The rich picture is normally used by system architect and ICT security experts to understand complex system. It was proposed by peter checkland as part of soft system methodology (SSM) [41]. A rich picture is one way of thinking holistically and builds intuitive consciousness that communicate more easily in perspective than words [42]. The rich picture may include people, Structures, sensors, machines Processes, Climate, Issues expressed by people, technology, Conflict and soon. Figure 4 elaborates the proposed requirement specification model for industry 4.0 framework.

8.2. Sub-System Delimitation

The next stage involves delimitation of the picture into important components, department, service, location or institution, technology, employment or applications. This can help in Identify the issue we need to address in large system by reorganizing various related component and identify relationships among key components according to specific perspective.

8.3. Requirement Elicitation

Requirement Elicitation is related to various ways used by software developer or security architect to gain facts about the system or project and define specific requirements. Requirements elicitation is the most challenging, error-prone and communication intensive stage of software development [42]. Requirement elicitation is user centric process. There are a number of requirements elicitation methods include Interviews, Brainstorming Sessions, Facilitated Application Specification Technique (FAST), Quality Function Deployment (QFD), Use Cases and many other methods [43].

8.4. Requirement Categorisation

Generally, Requirements for Industrial Internet of things application development and internal security design are becoming more complex and fragile because requirements are expected to integrate and support many technologies that cut across many multiple disciplines. In our model requirements are branded into two categories namely functional (for software development) and non-functional (security implementation) requirements.

8.4.1. Functional Requirement

Functional Requirement defines behaviour, features and functionality of the system. It describes a software system, application, modules or its component [44]. A functional requirement can be mathematical formulae, model of presentation, data manipulation, business process, user interaction, or any other specific functionality which defines what function a system is likely to perform. Functional Requirements are also called Functional Specification and can be divided in to transaction processing, business logic, reporting requirements, administrative functions, authorization levels, data administration and many others. In agile-driven project, functional requirements can be represented using software requirement document, use case, activity diagram, work break down (WBP), prototype and other models [44].

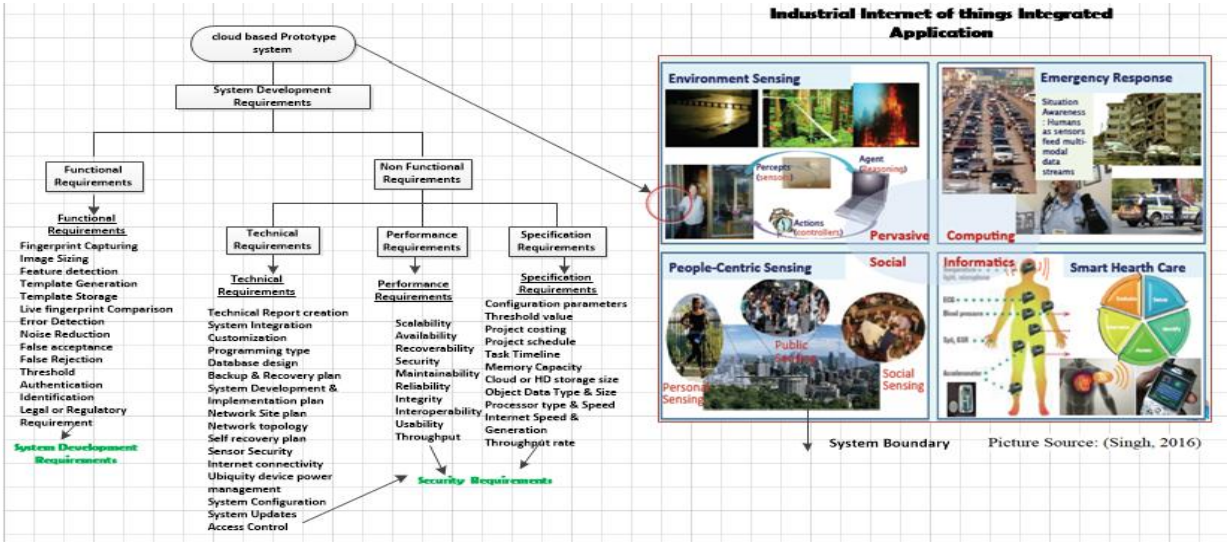

Figure 5. Component based Industrial Internet of things requirement specification model

8.4.2. Non - Functional Requirement

Non - functional requirements define the general quality aspects of the system and are sometimes referred to as quality attributes [45]. Generally, non-functional requirements states how the particular system must behave and establish framework of its functionality. In our proposed model, non-functional requirements are employed for IIoT security design and implementation.

Non-functional Requirements must support all the three key security services namely confidentiality, integrity and availability [8]. Though availability and integrity are two most important security attributes for industrial Internet of things or critical infrastructure [8]. Other security attributes include usability, reliability, performance and scalability.

8.5. Requirement Integration

Requirement Integration is the final stage in our proposed model. It involves the merging two or more diverse set of requirements either mono-directional or bi-directional so that the functionality can flow smoothly between two or more sub systems, processes or components [46]. Requirement or software integration can be conducted manually or by engaging special tools. Examples of these special tools include Mule Soft Any point Platform, IBM Enterprise BUS, Dell Boomi, APIGEE, Jitter bit, WSO2 and FUSE ESB [47].

9. Conclusions

Industry IoT technologies have been implemented in varieties of industries like health care, logistics, avionics, waste management, military, smart cities and many other fields under the auspice of industry 4.0 initiatives. Industry 4.0 frameworks have provided opportunities and challenges to software developer and ICT security architects for new IT solutions and innovation. There will be always a new demand for IT software re-organisation, customisation, upgrading and development of new application or security solutions to tap on available numerous opportunities. However, the complexity, diversity and blur nature in technological application makes the framework difficult to be understood. For this reason, the study have highlighted industry 4.0 key technological components, critical infrastructure, differences, relationships, industrial evolution, prospective, barriers and proposed component and function based model for requirement engineering process.

REFERENCES

[1] G. Kamieniecky and J. Bennet, “Emerging use of Industrial Internet of Things (IIoT),” 2019.

[2] L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, “A survey on internet of things and cloud computing for healthcare,” *Electron.*, vol. 8, no. 7, pp. 1–49, 2019.

[3] C. Qu, M. Tao, and R. Yuan, “A hypergraph-based blockchain model and application in internet of things-enabled smart homes,” *Sensors (Switzerland)*, vol. 18, no. 9, 2018.

[4] E. MOHAMAD *et al.*, “Review on Implementation of Industry 4.0 Globally and Preparing Malaysia for Fourth Industrial Revolution,” *Proc. Des. Syst. Conf.*, vol. 2018.28, no. 0, p. 2203, 2018.

[5] W. Aulbur, A. CJ, and R. Bigghe, “Skill Development for Industry 4.0,” *Rol. Berger. BRICS Ski. Dev. Work. Group, India Sect.*, pp. 1–50, 2016.

[6] J. Stephen Topper and N. C. Horner, “Model-based systems engineering in support of complex systems development,” *Johns Hopkins APL Tech. Dig. (Applied Phys. Lab.*, vol. 32, no. 1, pp. 419–432, 2013.

[7] L. Atzori, A. Iera, and G. Morabito, “Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm,” no. December, 2016.

[8] A. Sens, "Blockchain Engineering," *ERCIM News*, no. 110, 2017.

[9] P. Gokhale, O. Bhat, and S. Bhat, "(PDF) Introduction to IOT," *Int. Adv. Res. J. Sci. Eng. Technol.*, vol. 5, no. 1, pp. 41–44, 2018.

[10] R. Subha, "Biometrics in Internet of Things (IoT) Security," vol. 5, no. 5, pp. 37–42, 2017.

[11] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: An Overview," *Internet Soc.*, vol. 5, no. October 2015, pp. 1–50, 2015.

[12] G. Singh, "Cyber-physical systems and IoT," 2016.

[13] S. M. P. P. S. A. P. Keyur K Patel, "Internet of Things-IOT Definition articl," *Ijesc*, vol. 6, no. 5, p. 10, 2016.

[14] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, *Blockchain and iot integration: A systematic survey*, vol. 18, no. 8. 2018.

[15] K. K. Patel, S. M. Patel, and P. G. Scholar, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 1–10, 2016.

[16] R. Achary and J. Shaileshbhai, "Internet of Things: Essential Technology, Application Domain, Privacy and Security Challenges," *Int. J. Comput. Appl.*, vol. 157, no. 6, pp. 13–21, 2017.

[17] C. O. Turcu and C. E. Turcu, "Industrial internet of things as a challenge for higher education," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 55–60, 2018.

[18] E. Of *et al.*, "An Overview of Industry 4. 0: Definition, Components, and Government Initiatives," no. December, 2018.

[19] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," vol. 101, no. April, pp. 1–12, 2018.

[20] D. Sontag, industry IoT vs industry 4.0 vs industry 5.0?, Making Sense of the Trend, Medium, May, 8, 2018. [online]. Accessed on: December 20, 2019. Available: https://medium.com/the-industry-4-0-blog/industril-iot-vs-industry-4-0-vs-industry-5-0-a5f9541da036.

[21] C. World, "The Internet of Things: An Overview," no. October, 2015.

[22] C. Alcaraz, "Critical infrastructure protection: Requirements and challenges for the 21st Critical Infrastructure Protection: Requirements and Challenges for the 21st Century," no. January 2015, 2017.

[23] M. E. Davey, "CRS Report for Congress Received through the CRS Web Resolution," no. 391, pp. 1–6, 2009.

[24] T. Simon, "Critical Infrastructure and the Internet of Things," no. 46, 2017.

[25] J. M. Rogerson, "Reconfiguring South Africa's hotel industry 1990–2010: Structure, segmentation, and spatial transformation," *Appl. Geogr.*, vol. 36, pp. 59–68, Jan. 2013.

[26] J. Thangaraj and R. L. Narayanan, "Industry 1.0 to 4.0: the evolution of smart factories," no. January, 2019.

[27] P. Sund, "Opportunities in Japan Opportunities & Barriers To Implementation of Opportunities in," *Bus. Sweden Tokyo*, no. April, 2017.

[28] I. Ungurean, N. C. Gaitan, and V. G. Gaitan, "An IoT architecture for things from industrial environment," *IEEE Int. Conf. Commun.*, 2014.

[29] A. Alshehri and R. Sandhu, "Access control models for virtual object communication in cloud-enabled IoT," *Proc. - 2017 IEEE Int. Conf. Inf. Reuse Integr. IRI 2017*, vol. 2017-Janua, pp. 16–25, 2017.

[30] M.. Paridah, A. Moradbak, A.. Mohamed, F. abdulwahab taiwo Owolabi, M. Asniza, and S. H.. Abdul Khalid, "We are IntechOpen, the world ' s leading publisher of Open Access books Built by scientists, for scientists TOP 1 %," *Intech*, vol. i, no. tourism, p. 13, 2016.

[31] M. Blowers, J. Iribarne, E. J. M. Colbert, and A. Kott, "In conclusion: The future internet of things and security of its control systems," *Adv. Inf. Secur.*, vol. 66, pp. 323–355, 2016.

[32] M. Kinoshita, "JAPAN ON THE NEW INDUSTRIAL REVOLUTION (NIR): Direction and its global implication for inclusive and sustainable industrial development," no. March, 2019.

[33] K. D. Thoben, S. A. Wiesner, and T. Wuest, "'Industrie 4.0' and smart manufacturing-a review of research issues and application examples," *Int. J. Autom. Technol.*, vol. 11, no. 1, pp. 4–16, 2017.

[34] J. Nagy, J. Oláh, E. Erdei, D. Máté, and J. Popp, "The role and impact of industry 4.0 and the internet of things on the business strategy of the value chain-the case of hungary," *Sustain.*, vol. 10, no. 10, 2018.

[35] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, no. December, pp. 492–496, 2017.

[36] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *ACM Comput. Surv.*, vol. 50, no. 3, 2017.

[37] A. Ustundag and E. Cevikcan, "Industry 4.0: Managing The Digital Transformation," *Springer Ser. Adv. Manuf.*, no. January, pp. 1–283, 2018.

[38] Inayat Ali, Sonia Sabir, and Zahid Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," *Int. J. Comput. Sci. Inf. Secur. (IJCSIS),*, vol. 14, no. 8, pp. 456–466, 2016.

[39] J. P. Meltzer and N. Shenai, "The US-China Economic Relationship: A Comprehensive Approach," *SSRN Electron. J.*, 2019.

[40] B. Tekinerdogan, "IoT System Development Methods," pp. 137–155.

[41] P. Horan, "Using Rich Pictures in Information Systems Teaching," *1st Int. Conf. Syst. Think. Mangement, 2000*, vol. 1, pp. 257–262, 2000.

[42] S. Bell and S. Morse, "Rich pictures: A means to explore the 'sustainable mind'?," *Sustain. Dev.*, vol. 21, no. 1, pp. 30–47, 2013.

[43] D. Zowghi and C. Coulin, "Requirements elicitation: A survey of techniques, approaches, and tools," *Eng. Manag. Softw. Requir.*, pp. 19–46, 2005.

[44] S. Roberts, S. Roberts, and G. H. Sanders, "R EQUIREMENTS D OCUMENT Digitally signed by," pp. 1–55, 2015.

[45] L. Chung, "Non-Functional Requirements Non-Functional Requirements IEEE definition development and evaluate for the customer prior to NFRs: NFRs:," pp. 1–26, 2011.

[46] P. Dike, "The impact of workplace diversity on organisations Title: The Impact of Workplace Diversity on Organisations Supervisor (Arcada): SVEINN ELDON," pp. 1–59, 2013.

[47] J. Olsson and J. Liljegren, "Examining current academic and industry Enterprise Service Bus knowledge and what an up-to-date testing framework could look like," no. june, 2012.