ITEJ Juli-2020, Volume 5 Nomor 1 Page 37 - 50

PTIPD
IAIN SYEKH NURJATI CIREBON

ITEJ
Information Technology Engineering Journals
eISSN : 2548-2157

Url : https://syekhnurjati.ac.id/journal/index.php/itej
Email : itej@syekhnurjati.ac.id

ITEJ Information Technology Engineering Journals

A Survey Paper: Implementation of the Internet of Things in Industry

Andi Kurniawan
STMIK Kediri
Teknik Informatika
Andiks3421@gmail.com

Abstract— The use of the Internet of Things (IoT) has been widely developed in various fields of technology application. Using IoT can make it easier to build robust industrial systems and applications and provide visualization for the safety of industrial employees by taking advantage of the increasing number of radio frequencies, wireless devices, mobile devices and sensors. In understanding the development of IoT in the industry, the paper reviews the latest IoT research, a survey that compares the use of IoT from several existing papers, the main applications of IoT in the industry, and identifies trends and research challenges. The main contribution of this survey paper is to systematically summarize the current state of IoT in the industry.

Keywords *— Internet of Things; Industrial;IoT*

I. INTRODUCTION

The use of the Internet in the last 2 decades has provided enormous benefits for all people and organizations spread all over the world. The greatest benefit of the Internet is the ability to produce data and services in real time through the development of information systems. The emergence of systems everywhere is strongly supported by technological growth. This technology allows the system to work properly. One of the technologies is the Internet of Things (IoT) device. At this time, IoT's role is to bring benefits to the community while providing a way to expand perceptions and the ability to modify the environment around us[1]. IoT has significant potential in various industries of Environmental, Safety with high risk, and Health. In these industries, IoT-based applications are prepared to offer safe, reliable and efficient solutions because of their ability to provide information. IoT is a technology that connects information systems with communication. In general, IoT forms a network to uniquely identify objects, collect data from the environment through various sensors, operate and interact physically to process the data that has been collected, and use the Internet to communicate and analyze data to determine further services[2]. In addition, IoT can predict through machine learning algorithms to facilitate planning, decision making for industry owners, and make a policy of what to do.

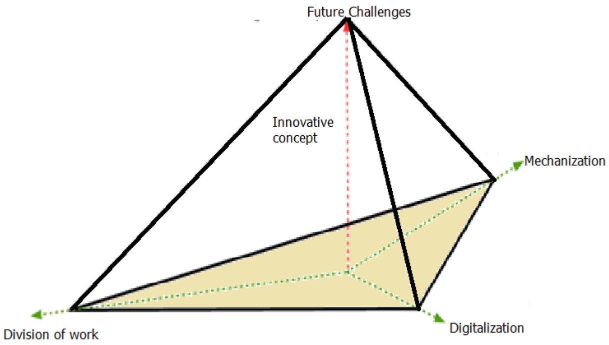

Figure 1. Future Industrial Strengths

Figure 1 shows the relationship of forces relevant to the current appearance and future evolution of the industry. Because of its age, the division of labor is the most influential force, followed by mechanization. Together with the newly added factor, namely digitalization, these three factors are the basis for the concept of industrial realization in the future.

With the application of IoT, low-cost electronic devices can increase the interaction between computing and software available on the Internet. In short, IoT can be an important tool in the coming years in the industrial world. The use of IoT can help people who interact in industries such as suppliers, technicians, distributors, business people, and consumers. By using IoT to connect devices, it is expected to make industrial production smarter and more efficient. In addition to improving operations, IoT also offers innovative solutions such as the creation of new business models such as the sale of goods can be augmented by services related to the assistance of data generated by IoT and real-time connectivity. However, adopting IoT in the industry will face several challenges including (1) Energy Efficiency, (2) Communication and challenges related to data connectivity and standardization, (3) Scalability (network size and interoperability) and (4) Security and Reliability.

By utilizing IoT, researchers intend to design analytical reports related to the benefits of using IoT in industry.

IoT can be considered a global network infrastructure company with many connected devices that rely on sensory, communication, networking, and information processing technologies. The basic technology for IoT is RFID technology, which allows microchips to send identification information to the reader via wireless communication. By using RFID readers, people can identify, track, and monitor every object that is attached with an RFID tag automatically. Another basic technology for IoT is the wireless sensor network (WSN), which mainly uses smart interconnected sensors to sense and monitor. Applications include environmental monitoring, health care monitoring, industrial monitoring, traffic monitoring, and so on. Advances in RFID and WSN significantly contributed to the development of IoT. In addition, many other technologies and devices such as barcodes, smart phones, social networks, and computers are used for comprehensive networking to support IoT (see Figure 2).

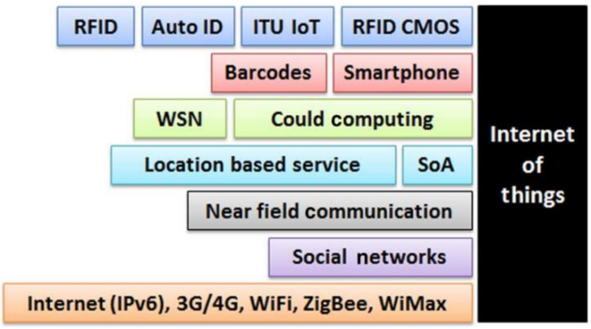

Figure 2. Technology related to IoT

So far, IoT has gained traction in industries such as logistics, manufacturing, retail and pharmaceuticals. With advancements in wireless communications, smartphones, and sensor network technology, more and more networks or smart objects are involved in IoT.

To provide high quality services to end users, IoT technical standards need to be designed to define specifications for the exchange of information, processing, and communication between various things. The success of IoT depends on standardization, which provides interoperability, compatibility, reliability and effective operations on a global scale. Many countries and organizations are interested in developing IoT standards because they can bring extraordinary economic benefits in the future.

Smart and connected IoT elements require the right technological infrastructure. This infrastructure is represented as a "technology stack" and is shown in Figure 3. The technology stack facilitates the exchange of data between assets and users, integrates data from business systems and external sources, functions as a platform for data storage and analysis, runs applications, and protects access to assets and data. The bottom half of the technology stack illustrates the elements associated with assets. There are two parts of software and hardware. One of the ongoing evolution is the addition of embedded sensors, RFID tags, and processors built into assets. Collectively, this allows new data to be collected. This data needs to be sent, and hence network connectivity, as shown in the middle block, is the main feature of IoT. Data collected and sent must be stored and processed in an efficient and interpretable manner. This is increasingly being done using cloud computing services, represented by the top blocks in the technology stack. Users are displayed at the top of the image, including those who access the results of the analysis as well as those involved in developing and maintaining the stack of technology elements and the models they support. Blocks on both sides of the stack identify the importance of authentication and security at all levels in the technology stack as well as the potential links with other systems and sources information.

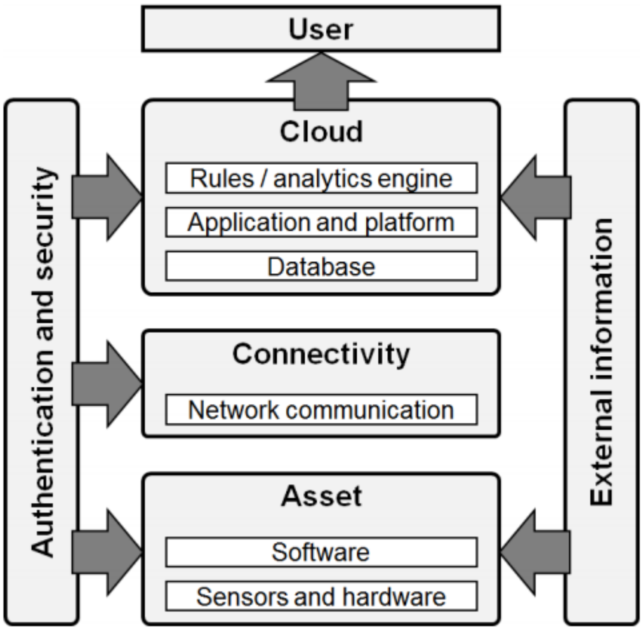

Figure 3. The stack technology to support IoT

II. SURVEY

IoT can be connected to everything that is connected to the Internet network. At this time, IoT has been used in various sectors, one of which is the industrial sector. The following is shown in Table 1 which provides a survey of research related to the use of IoT in the industry. The survey does not fully cover the IoT aspects especially the specific aspects. The survey emphasizes the application of using IoT in industry. Most of the IoT research in the table deals exclusively with the use of IoT in industries that focus on a particular field or challenge. Some pure surveys concentrate on IoT and related tools, while others discuss the challenges of IoT in the industry going forward in carrying out certain tasks. Quality improvement will always be discussed if it relates to the use of IoT tools. IoT is used as a media for decision making what will be done after a problem occurs. This survey not only provides a comprehensive study of research contributions using IoT, but also presents the latest solutions that can be utilized in the analysis of IoT data in the industry. The solutions presented are expected to be useful solutions for the future development of the industry. In several studies have conducted trials with better results than previous studies or new research that has never been done.

Table 1. Research surveys related to the use of IoT in the industry

Researcher	Year	Area of Interest	Description
Sven Plaga, at al [8]	2018	• Industrial • Internet of Things (IoT) • Cyber Security • Smart Environments • Decentralisation • Secure Communications	One important aspect of modern IoT infrastructure is decentralized communication, often called Peer-to-Peer (P2P). In the context of industrial communication, P2P contributes to the resilience and increased stability for industrial components. Today's industrial facilities are still dependent on a centralized network scheme that is considered mandatory to meet security standards. In order to succeed, the industry introduces P2P technology to maintain the current level of protection and also consider the possibility of new threats.
Hairong Yan, at al [11]	2017	• Industrial real-time control • Internet of Things (IoT) • Mixed time-triggered mode • Event-triggered mode	For real-time control in an industrial environment, IoT controllers in an industry can play an important role in it. But in the IoT environment, every industrial controller is required to obtain effective information from all types of sensors in real-time. Communication between industrial IoT controllers and sensors must delay lower time. New design methods are proposed for time-triggered industries and mixed event controllers for real-time industrial control in an IoT environment.
Montbel Thibaud, at al [9]	2018	• Healthcare • IoT • Environment Health and Safety (EHS) • Food Supply Chain • Connected Vehicles • Smart City	A review of some of the research that has been published using IoT-based applications in the high-risk EHS industry with particular emphasis on the health industry, food supply, the mining and energy industry, smart transportation (eg connected vehicles), and building & infrastructure management for operations emergency response until 2016.
Jesus Martin Tavalera, at al [5]	2017	• Agro-Industry • IoT • Environment monitoring	The review reviews agro-industry and environmental applications that use the Internet of Things (IoT). Selected references are grouped into four application domains that

		- SLR	correspond to: monitoring, control, logistics, and prediction. Specific details of the implementation of each selected reference are compiled to make distributions using sensors, actuators, resources, edge computing modules, communication technologies, storage solutions, and visualization strategies.
Min Wei, at al [10]	2015	- IoT - Information Model - Energy Efficiency - Integrated Energy Systems	Research to present an IoT-based communication framework with a general information model facilitates the development of energy management systems for industrial customers. In addition, the study also developed and implemented an IoT-based energy management platform on the general information model and open communication protocol, which utilizes the integration of energy supply networks to implement energy management in industrial facilities. The results show that the proposed platform can not only increase entity interconnectivity in industrial energy management systems but also reduce the energy costs of industrial facilities.
Shamsul Huda, at al [3]	2018	- IoT - Industrial control systems (ICS) - Critical Infrastructure - Supervisory Control and Data Acquisition (SCADA) Network	The SCADA-based ICS network is integrated with the company's network via the internet. Therefore devices from the SCADA network face significant threats from malicious attacks either through corporate network vulnerabilities or the devices used in SCADA. Traditional IT security software products are not enough for ICS. The study proposes a secure architecture for ICS networks which proposes a malware detection model based on SCADA network traffic.
Daeil Kwon, dkk [4]	2016	- IoT - Maintenance - System Health Management	Prognostic and System Health Management (SHM) sensors may be used to assess system health, diagnose anomalous behavior, and predict useful residual performance over the life of the asset. The rise of the Internet of Things (IoT) allows SHM to be applied to all types of assets in all sectors, thus creating a paradigm shift that opens up new business opportunity opportunities.
Saad Mubeen, at al [7]	2017	- IoT - Fog Computing - Cloud Computing - Industrial Automation Systems	The research investigates the interaction of Cloud Computing, Fog Computing, and the Internet of Things (IoT) in application controls that target industrial automation. In this context, a prototype was developed to explore the use of IoT devices that communicate with cloud-based controllers, e.g., controllers are used in cloud computing or fog.
Eshrat E Alahi, dkk	2017	- IoT - Agricultural	Research designs and develops smart nitrate sensors to monitor nitrate concentrations in

[41]		Industry • Nitrate Detection	surface and ground water. This system is able to send data directly to an IoT-based web server, which will be useful for developing a distributed monitoring system in the future. The developed system has the potential to monitor the impact of industrial, agricultural, or urban water quality activities, in real time.
Patrick McNeil [6]	2018	• IoT • Cement Industry	The Cement Industry has utilized IoT to exert system control and improve the visibility and efficiency of system production. The Cement Industry Automation has made production consistency and efficiency. Automation through IoT can provide safety for cement factory employees. In addition, IoT can check temperatures suitable for manufacturing cement products that meet the required standards
Santiago Egea, dkk [42]	2018	• IoT • Industry • Emergency Detection • Machine Learning	IoT in the industry makes it possible to separate and prioritize multimedia related sensor data. With this separation, the sensor is able to detect emergency situations efficiently and avoid material and human damage. This can improve the model's accuracy and execution time.
Hussein Khaleel, dkk [39]	2017	• IoT • Industry • Transportation • Immune Genetic Algorithm	Usage from IoT was tested, including wireless sensors and network actuators for the machine monitoring industry and identification-based radio frequency systems for operator management, placement, and authorization. IoT to visualize real-time information from the device. This research illustrates the development of prototypes in the car manufacturing industry.
Yingchen Wang, dkk [40]	2018	• IoT • Industry • Transportation • Immune Genetic Algorithm	IoT techniques provide more information for inventory control. With increasing economic competition, the supply of materials is at the core of the company. The study considers the supply of supplies consisting of several suppliers, manufacturers, and several distributors. The immune genetic algorithm effectively overcomes deficiencies previous genetic algorithms, improved global search capabilities and search efficiency.

III. KEY OF IOT TECHNOLOGY

A. Technology for tracking and identifying

Identification and tracking technology on IoT using RFID, barcode and smart sensor systems. Simple RFID systems consist of RFID readers and RFID tags. Because of its ability to identify, track, and track devices and physical objects, RFID systems are increasingly being used by industries, such as logistics, supply chain management, and health service monitoring

[12], [15]. Other benefits of an RFID system are to provide precise real-time information about the devices involved, reduce labor costs, simplify business processes, improve the accuracy of inventory information, and improve business efficiency. So far, RFID systems have been used successfully by various manufacturers, distributors, and retailers in many industries [13], [14]. The latest development of RFID technology is focused in the following aspects [12], [13], [14], [15]: 1) active RFID system with spread-spectrum transmission; and 2) RFID Application management technology [13], [14].

The growth of RFID-based applications still needs a lot of time [16]. To further promote RFID technology, RFID can be integrated with WSN to track events in real time. In particular, emerging wireless intelligent sensor technologies, such as electromagnetic sensors, biosensors, off-board sensors, sensor tags, independent tags, and device sensors further facilitate the implementation and deployment of industrial services and applications. By integrating data obtained by smart sensors with RFID data, IoT is the most suitable tool for industrial environments.

B. Communication technology on IoT

IoT can contain many electronic devices, cellular devices, and Industrial equipment. Different things have different communications, networks, data processing, data storage capacity, and transmission power. For example, there are now many smart phones for strong communication, networking, data processing and data storage capacity. Compared to smart phones, heart rate monitor watches only have limited communication and computing capabilities. All of these things can be connected with network and communication technology.

IoT involves several networks such as WSN, wireless network, WLAN, etc. This network helps in the exchange of IoT information. The gateway has the ability to facilitate communication or interaction of various devices via the Internet. Gateways can also utilize network knowledge by executing optimization algorithms locally. Therefore, the gateway can be used to handle many complex aspects involved in communication on the network [16].

C. The network used for IoT

IoT can consist of various electronic devices, cellular devices, and Industrial equipment. There are several protocols for wireless networks to work such as Wireless Sensors and Network Actuators (WSAN) or Ad Hoc Networks (AHNs) [29]. However, the network must be reviewed first before it can be applied to IoT. The reason is because in IoT often has communication and various computing capabilities, and various QoS requirements. In contrast, nodes in WSNs usually have the same requirements for hardware and network communications. In addition, the IoT network uses the Internet to support information exchange and data communication. In contrast, WSN and AHN do not have the ability to engage the Internet in communication.

IV. IOT APPLICATIONS IN INDUSTRIES

The IoT application is still in its early stages, but the use of IoT has been growing rapidly and is developing. Several IoT applications are being developed and used in various industries including environmental monitoring, health care services, inventory and production management, food supply, transportation, workplace and home support, security, and surveillance. The design of the industrial IoT application needs to consider various objectives. Depending on the intended industrial application, the designer may have to trade off between these goals to achieve a balance of costs and benefits. Below are some IoT applications in the industry.

1. Using IoT in the health care industry [17].

IoT provides new opportunities to improve health services. Monitoring can be carried out continuously and supported by identification, sensing, and communication capacity, all objects in the health service system (people, equipment, medicines, etc.) [18]. Enabled by global connectivity, all information related to health care (logistics, diagnosis, therapy, recovery, treatment, management, finance, and even daily activities) can be collected, managed and shared efficiently. For example, a patient's heart rate can be collected by sensors from time to time and then sent to the doctor's office. By using personal computing devices (laptops, cellphones, tablets, etc.) and cellular internet access (WiFi, 3G, LTE, etc.), IoT-based health services can be both mobile and personal [19]. The expansion of cellular internet services has accelerated the development of home health services supported by IoT services.

2. Using IoT in the supply of food ingredients [20].

Food supply is currently very distributed and complex. Each region has a large geographical area, complex operational processes, and a large number of stakeholders. Complexity has caused many problems in quality management, operational efficiency, and public food safety. IoT technology offers promising potential to overcome the challenges of traceability, visibility and control. This can cover Food Supply from the right agriculture, to food production, processing, storage, distribution and consumption. Food supply is safer, more efficient and sustainable in the future. A typical IoT solution for Food Supply (called Food-IoT) consists of three parts: a) field devices such as WSN nodes, RFID readers / tags, user interface terminals, etc .; b) backbone systems such as databases, servers, and many types of terminals connected by network-distributed computers, etc .; and c) communication infrastructure such as WLAN, cellular, satellite, power lines, Ethernet, etc. Like the IoT system which offers network capacity everywhere, all of these elements can be distributed throughout the Food Supply. In addition, IoT also offers effective sensing functionality to track and monitor the food production process. Large amounts of raw data can be further processed and analyzed to improve business decision-making processes and support.

3. Using IoT for safer mining production. Mining safety is a major problem that needs attention for many countries due to working conditions in underground mines. To prevent and reduce accidents in mines, IoT technology is used to sense early warning signals for disasters, predict disasters, and increase safety of underground production [21]. By using RFID, WiFi, and other wireless technologies and communication devices allowing for effective communication between surface and underground, mining companies can track the location of underground miners and analyze critical safety data collected from sensors to increase security measures. Another useful application is sensors for chemicals and biologics for early disease detection and diagnosis of underground miners, such as those working in dangerous environments. Chemical and biological sensors can be used to obtain biological information from the body and human organs and to detect harmful dust, harmful gases, and other environmental hazards that can cause accidents. The challenge is that wireless devices require power and have the potential to blow up gas in a mine. More research is needed regarding the safety characteristics of IoT devices used in mining production.

4. Using IoT in transportation and logistics.

IoT will play an increasingly important role in the transportation and logistics industry. More and more physical objects equipped with bar codes, tags or RFID sensors, transportation and logistics companies can carry out real-time monitoring of the movement of physical objects from origin to destination throughout the supply chain including manufacturing, shipping, distribution, and so on [22]. In addition, IoT is expected to offer a promising solution to change the transportation system and car services [23]. Because vehicles have increasingly strong sensing, networks, communications, and data processing, IoT technology can be used to improve capabilities and share underutilized resources between vehicles in parking lots or on the road. For example, IoT Technology makes it possible to track every vehicle, existing location, monitor its movements, and predict future locations [24], [25]. Security and privacy protection are important for the wide use of IoT in transportation and logistics, today many vehicle drivers are worried about leakage of personal information [26]. Reasonable efforts in technology, law and regulation are needed to prevent unauthorized persons from accessing their personal data.

5. Using IoT to detect fires. IoT has been used in the field of fire safety to detect potential fires and provide early warning for possible catastrophic fires. RFID tags and barcodes are attached to fire fighting products to develop national database information and management systems [27]. By utilizing RFID tags, cellular RFID readers, smart video cameras, sensor networks, and wireless communication networks, related organizations can carry out automatic diagnoses to realize real-time environmental monitoring, early fire warnings and emergency rescue as needed [28].

V. CHALLENGES AND FUTURE TRENDS

It is widely accepted that IoT technology and applications are still in its infancy. There are still many research challenges for industrial use such as technology, standardization, security and privacy. Future efforts are needed to overcome these challenges and examine the characteristics of different industries to ensure the compatibility of IoT devices in the industrial environment. An adequate understanding of industry characteristics and requirements on factors such as cost, security, privacy and risk is required before IoT is widely accepted and used in industry.

A. Technical Challenges

Although much research efforts have been made on IoT technology, there are still technical challenges.

1) From a network point of view, IoT is a very complex heterogeneous network, including connections between various types of networks through various communication technologies. At present, there is a general lack of a widely accepted platform that hides the heterogeneity of network / communication technology and provides transparent naming services for various applications. Large amounts of data transmission across the network at the same time can also cause frequent problems of delay, conflict, and communication. This is a challenge to develop network technologies and standards that allow data to be collected by a large number of mobile devices efficiently in an IoT network. Managing matters that are connected in terms of facilitating collaboration between different entities and administrative tools addressing, identifying, and optimizing at the architecture and protocol level is a research challenge.
2) From a service standpoint, the lack of a generally accepted service description makes service development and integration of physical object objects into value-added

services more difficult. The services developed cannot match different communication and implementation environments. In addition, robust service discovery methods and service naming objects need to be developed to deploy IoT technology.

3) IoT is often developed based on the traditional Information and Communication Technology environment and is influenced by everything that is connected to the network, this is used to integrate IoT with existing IT systems into an integrated information infrastructure. Furthermore, with things that are connected to the Internet with a very large amount, a large amount of real-time data flow will be automatically produced by the things that are connected. Data may not have much meaning value unless people find effective ways to analyze and understand it. Analyzing or processing massive amounts of data generated from IoT applications and existing IT systems to obtain valuable information requires strong big data analytics skills, which can be challenging for many end users. In addition, integrating IoT devices with external resources such as existing software systems and web services requires the development of various middleware solutions, because applications vary greatly across industries. Building practical applications that are heterogeneous with related data, IoT can be combined with data for various industries.

B. Standardization

The rapid growth of IoT makes standardization difficult. However, standardization plays an import role for the further development and deployment of IoT. Standardization at IoT aims to reduce entry barriers for new service providers and users, to improve the interoperability of various applications / systems and to enable products or services to work better at a higher level. A careful standardization process and a lot of coordination of efforts are needed to ensure that devices and applications from various countries are able to exchange information. The various standards used in IoT (eg, security standards, communication standards, and identification standards) may be key to the spread of IoT technology and need to be designed to embrace emerging technologies. Specific problems with IoT Standardization include interoperability issues, access level radio issues, semantic interoperability, and security and privacy issues. In addition, industry specific guidelines or standards for implementing IoT in an industrial environment need to be recommended for easier integration of various services.

C. Information Security and Privacy Protection

The acceptance and deployment of new IoT technology and most services will depend on information security and privacy protection data, which are two difficult problems in IoT because of its deployment, mobility, and complexity. Many existing technologies are available for consumer use, but are not suitable for industrial applications that have strict safety and security requirements. To secure information, encryption technology borrowed from other networks needs to be carefully reviewed, when used to build IoT. IoT allows many things in everyday life to be tracked, monitored and connected, and a lot of personal and personal information can be collected automatically. Protecting IoT privacy in the environment becomes more serious than traditional ICT environments because the number of attack vectors on IoT entities appears to be much greater. For example, a health monitor will collect patient information, such as heart rate and blood sugar levels and then send information directly to the doctor's office through a network. When the information is transferred through the network, patient data can be stolen or compromised. Another example is the bio-sensor used in the food industry can be used to monitor temperature and bacterial composition of food stored in refrigerators. When food decays, data can be sent back to the food company through the network. However, the data must be kept in strict confidence to protect the reputation of the food company. It should be noted that some issues, such as the definition of privacy and legal interpretation are still vague and not clearly defined in IoT. Although there is already network security technology providing a basis for privacy and security at IoT, further work still needs to be done. Reliable security protection mechanisms for IoT need to be examined from the following aspects: 1) security and privacy from a social, legal and cultural perspective; 2) mechanism of trust and reputation; 3) communication security such as end-to-end encryption; 4) privacy of communication and user data; and 5) security of services and applications.

D. Research Trends

The development of the IoT infrastructure will likely follow an additional approach and develop from the identification of existing techniques, such as RFID. International collaborative efforts and system-level perspectives are needed to tackle IoT related challenges. In addition to conducting research to overcome the challenges above, it is also necessary to identify several other research trends.

1) Integrating Social Networks With IoT Solutions: It is possible to use social networks to improve communication between various IoT matters [30]. There is a trend for a move from IoT to a new vision called Web of Things, this allows IoT objects to become active actors and partners on the Web.

2) Developing Green IoT Technology: As it involves billions of connected IoT sensors that communicate via wireless networks, sensor power consumption is enormous and limitations for IoT deployment. Saving energy must be a critical design target for IoT devices, such as wireless sensors. There is a need to develop energy efficient techniques or approaches that can reduce the power consumed by sensors [31].

3) Developing Context-Aware IoT Middleware Solutions: When billions of sensors are connected to the Internet, it turns out that it is not feasible for people to process all the data collected by IoT sensors. Context-Aware computing techniques, such as IoT middleware, are proposed to better understand sensor data and help decide what data needs to be processed. At present, most IoT middleware solutions do not have Context-Aware capabilities [32].

4) Employ Artificial Intelligence Techniques (AI) to Make Smart Objects or Smart Objects :. Future IoT systems must have characteristics including "self-configuration, self-optimization, self-protection, and self-healing" [33], [34]. Smart objects will become smarter and more conscious with greater memory, processing, and reasoning abilities in the future [35].

5) Combining IoT and Cloud Computing: Cloud Computing provides a good way to connect and allows us to access different things on the internet. Further research will focus on implementing new models or platforms that provide "service" to Cloud Computing [36], [37], [38].

VI. CONCLUSION

IoT integrates a variety of devices equipped with sensing, identification, processing, communication, and network capabilities. In particular, robust sensors are cheaper and smaller, which makes their use everywhere. The industry has a strong interest in using IoT devices to develop industrial applications such as automatic monitoring, control, management and maintenance. Due to rapid advances in industrial technology and infrastructure, IoT is expected to be widely applied to the industry. For example, the food industry integrates WSN and RFID to build automated systems for tracking, monitoring, and tracking food quality along the food supply chain to improve food quality. This paper reviews the latest research on IoT from an industry perspective. This paper focuses on the application of IoT to the industry and highlights the challenges and possibilities for research in the industry.

REFERENCES

[1] S. Saluky, “Development of Enterprise Architecture Model for Smart City”, itej, vol. 2, no. 2, pp. 12 - 18, Dec. 2017.

[2] Y. Marine and S. Saluky, “Penerapan IoT untuk Kota Cerdas”, itej, vol. 3, no. 1, pp. 36 - 47, Jul. 2018.

[3] Huda, S., Yearwood, J., Mehedi, M., and Almogren, A. (2018): Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks, Applied Soft Computing Journal, 71, 66–77. https://doi.org/10.1016/j.asoc.2018.06.017

[4] Kwon, D., and Hodkiewicz, M. R. (2016): IoT-Based Prognostics and Systems Health Management for Industrial Applications, IEEE Access, 4, 3659–3670. https://doi.org/10.1109/ACCESS.2016.2587754

[5] Martín, J., Eduardo, L., Alejandro, J., Alejandra, M., Manuel, J., Teresa, D., Alfredo, L., Hoyos, A., and Ernesto, L. (2017): Review of IoT applications in agro-industrial and environmental fields, 142(118), 283–297. https://doi.org/10.1016/j.compag.2017.09.015

[6] Mcneil, P. (2018): Secure Internet of Things Deployment in the Cement Industry, IEEE Industry Applications Magazine, 24(October 2017), 14–23. https://doi.org/10.1109/MIAS.2017.2739833

[7] Mubeen, S., Member, S., Nikolaidis, P., Didic, A., Pei-breivold, H., Sandström, K., and Behnam, M. (2017): Delay Mitigation in Offloaded Cloud Controllers in Industrial IoT, 5. https://doi.org/10.1109/ACCESS.2017.2682499

[8] Plaga, S., Wiedermann, N., Duque, S., Tatschner, S., Schotten, H., and Newe, T. (2019): Securing future decentralised industrial IoT infrastructures : Challenges and free open source solutions, Future Generation Computer Systems, 93, 596–608. https://doi.org/10.1016/j.future.2018.11.008

[9] Thibaud, M., Chi, H., Zhou, W., and Piramuthu, S. (2018): Internet of Things (IoT) in high-risk Environment , Health and Safety (EHS) industries : A comprehensive review, Decision Support Systems, 108, 79–95. https://doi.org/10.1016/j.dss.2018.02.005

[10] Wei, M., Ho, S., and Alam, M. (2016): An IoT-based energy-management platform for industrial facilities, Applied Energy, 164, 607–619. https://doi.org/10.1016/j.apenergy.2015.11.107

[11] Yan, H., Jun, L., Zhi, P., Yue, X., and Su, H. (2018): Journal of Industrial Information Integration Mixed time-triggered and event-triggered industrial controller in IoT environment, Journal of Industrial Information Integration, 11, 11–18. https://doi.org/10.1016/j.jii.2017.06.004

[12] X. Jia, O. Feng, T. Fan, and Q. Lei, “RFID technology and its applications in internet of things (IoT),” in Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet), Yichang, China, Apr. 21–23, 2012, pp. 1282–1285.

[13] C. Sun, “Application of RFID technology for logistics on internet of things,” AASRI Procedia, vol. 1, pp. 106–111, 2012.

[14] E. W. T. Ngai, K. K. Moon, F. J. Riggins, and C. Y. Yi, "RFID research: An academic literature review (1995–2005) and future research directions," Int. J. Prod. Econ., vol. 112, no. 2, pp. 510–520, 2008.

[15] M. K. Lim, W. Bahr, and S. Leung, "RFID in the warehouse: A literature analysis (1995–2010) of its applications, benefits, challenges and future trends," Int. J. Prod. Econ., vol. 145, no. 1, pp. 409–430, 2013.

[16] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "IoT gateway: Bridging wireless sensor networks into internet of things," in Proc. IEEE/IFIP 8th Int. Conf. Embedded Ubiquitous Comput. (EUC), Hong Kong, China, Dec. 11–13, 2010, pp. 347–352.

[17] Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, "Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in Proc. 2013, 15th Int. Conf. Adv. Commun. Technol. (ICACT), Pyeongchang, Korea, pp. 529–534.

[18] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," Comput. Netw., vol. 54, no. 15, pp. 2688–2710, 2010.

[19] I. Plaza, L. Martín, S. Martin, and C. Medrano, "Mobile applications in an aging society: Status and trends," J. Syst. Softw., vol. 84, no. 11, pp. 1977–1988, 2011.

[20] Z. Pang, Q. Chen, W. Han, and L. Zheng, "Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion," Inf. Syst. Front., to be published.

[21] Q. Wei, S. Zhu, and C. Du, "Study on key technologies of internet of things perceiving mine," Procedia Eng., vol. 26, pp. 2326–2333, 2011.

[22] B. Karakostas, "A DNS architecture for the internet of things: A case study in transport logistics," Procedia Comput. Sci., vol. 19, pp. 594–601, 2013.

[23] H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligent transportation system based on the internet of things," Commun. Comput. Inf. Sci., vol. 312, pp. 572–580, 2012.

[24] E. Qin, Y. Long, C. Zhang, and L. Huang, "Cloud computing and the internet of things: Technology innovation in automobile service," LNCS 8017, New York, NY, USA, 2013, pp. 173–180.

[25] Y. Zhang, B. Chen, and X. Lu, "Intelligent monitoring system on refrigerator trucks based on the internet of things," Wireless Commun. Appl., vol. 72, pp. 201–206, 2012.

[26] C. G. Keller, T. Dang, H. Fritz, A. Joos, C. Rabe, and D. M. Gavrila, "Active pedestrian safety by automatic braking and evasive steering," IEEE Trans. Intell. Transp. Syst., vol. 12, no. 4, pp. 1292–1304, Dec. 2011.

[27] Y. C. Zhang and J. Yu, "A study on the fire IOT development strategy," Procedia Eng., vol. 52, pp. 314–319, 2013.

[28] Z. Ji and A. Qi, " The application of internet of things (IOT) in emergency management system in China," in Proc. 2010 IEEE Int. Conf. Technol. Homeland Security (HST), pp. 139–142.

[29] C. Han, J. M. Jornet, E. Fadel, and I. F. Akyildiz, "A cross-layer communication module for the internet of things," Comput. Netw., vol. 57, no. 3, pp. 622–633, 2013.

[30] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT)-when social networks meet the internet of things: Concept, architecture and network characterization," Comput. Netw., vol. 56, no. 16, pp. 3594–3608, 2012.

[31] E. Yaacoub, A. Kadri, and A. Abu-Dayya, "Cooperative wireless sensor networks for green internet of things," in Proc. 8th ACMSymp. QoS Security Wireless Mobile Netw., Paphos, Cyprus, 2012, pp. 79–80.

[32] Arman Nuradi, "Pengembangan Arsitektur Otomatisasi Smart Home dengan Internet of Things", JSC, vol. 1, no. 2, pp. 51 - 61, Dec. 2018.

[33] Aditya Kurniawan, Ratna Mayasari, and Muhammad Ary Murti, "Implementation of Cryptographic Algorithm on IoT Device's ID", JSC, vol. 1, no. 2, pp. 20 - 28, Dec. 2018.

[34] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, “Smart objects as building blocks for the internet of things,” IEEE Internet Comput., vol. 14, no. 1, pp. 44–51, Jan./Feb. 2010.

[35] Y. Ding, Y. Jin, L. Ren, and K. Hao, “An intelligent self-organization scheme for the internet of things,” IEEE Comput. Intell. Mag., vol. 8, no. 3, pp. 41–53, Aug. 2013.

[36] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, “Cloud computing for internet of things & sensing based applications,” in Proc. 2012 6th Int. Conf. Sens. Technol. (ICST), Kolkata, West Bangal, India, pp. 374–380.

[37] S. Fang, L. Xu, H. Pei, and Y. Liu, “An integrated approach to snowmelt flood forecasting in water resource management,” IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 548–558, Feb. 2014.

[38] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (IoT): A vision, architectural elements, and future directions,” Future Gen. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[39] Khaleel, H., Conzon, D., Kasinathan, P., Brizzi, P., Pastrone, C., Pramudianto, F., Eisenhauer, M., Cultrona, P. A., Rusinà, F., and Luká ˇ, G. (2017): Heterogeneous Applications , Tools , and Methodologies in the Car Manufacturing Industry Through an IoT Approach, 11(3), 1412–1423.

[40] Wang, Y., Geng, X., Zhang, F. A. N., and Ruan, J. (2018): An Immune Genetic Algorithm for Multi-Echelon Inventory Cost Control of IOT Based Supply Chains, IEEE Access, 6, 8547–8555. https://doi.org/10.1109/ACCESS.2018.2799306

[41] Alahi, E. E., Member, S., Xie, L., Mukhopadhyay, S., and Burkitt, L. (2017): A Temperature Compensated Smart Nitrate-Sensor for Agricultural Industry, 64(9), 7333–7341..

[42] Egea, S., Mañez, A. R., Carro, B., Sánchez-esguevillas, A., Member, S., Lloret, J., and Member, S. (2018): Intelligent IoT Traffic Classification Using Novel Search Strategy for Fast-Based-Correlation Feature Selection in Industrial Environments, 5(3), 1616–1624. https://doi.org/10.1109/JIOT.2017.2787959