Beneficial Impact of Internet of Things in Business – A Critical Review

Dr. S. Saiganesh  
Dy. Director, Dayananda Sagar Business School, Bangalore  

Prof. Kaveri C.S.  
Assistant Professor, AIMS-IBS, Bangalore

Abstract

The Internet of things (IoT) assigns actual substances (or gatherings of such materials) that are circled with gadgets, taking care of capacity, programming, other than other aptitude that connection and trade realities utilizing different devices and frameworks with the assistance of Internet or other correspondence conditions. The region has advanced because of the converging of complex innovations, containing plentiful processing, item sensors, continuously noticeable inserted frameworks, other than AI. Standard fields of installed frameworks, remote gadget joins, controller frameworks, robotization (including home and development mechanisations), independently and commonly enabling the Internet of Things. IoT innovation is identical to items concerning the possibility of the “savvy homes”, with gadgets (like light fittings, indoor regulators, home security gadgets then observation cameras, other than other domestic devices) that contrary energies at least one shared ecologies, likewise can be arranged by means of contraptions that are interconnected with the organization, as cell phones notwithstanding brilliant speakers. The IoT could be used even in medical services associations too with which the illnesses can be spotted and suitable therapy gave to the patients. By the by, the IoT isn’t liberated from gambles being developed of this exact advancements and items, explicitly with regards to the part of protection and security worries and subsequently the public authority and modern moves have likewise begun, thinking about the improvement of worldwide and nearby benchmarks, proposals and administrative designs. This specific paper gives a more extensive comprehension of the IoT idea concerning how the headway in innovation has changed the different areas in the general public to adjust to connect themselves with the implanted programming. Important benefits given by IoT have been pondered exhaustively. How much the advantages are being valued by different ventures overall are likewise pondered.

Keywords: Internet of Things, Technology, Automation, Embedded Technology, Software Privacy

Introduction

The world has arrived at that time of presence wherein essentially every individual is dependent on the Internet. Advancement of Internet period took another structure wherein the entire of the planet might be interfacing among one another and such an age is known as IoT (Internet of Things). The previously mentioned is a gigantic idea
that is advancing every day other than the potential outcomes in IoT is boundless. The assortment of net suppliers, clients and the web contributions inside the contraptions are expanding step by step possibly they are associated through wires or with the assistance of wi-fi. Any individual can exploit a few information exactly readily available. Prior to the revelation of IoT, there have been best assortments of correspondence the two people to people or people to contraptions, yet the development of IoT made it conceivable to lay out report among machines to machines (M2M). The possibility of IoT traces all the way back to 1982 in which a coke gadget became changed and equipped for associating with the net. The contraption produced a report of the fluids regardless of whether the fluids were bloodless. The main thought at the rear of the Internet of Technology is to adjust data between genuine global articles around us, with the help of primary innovations like RFID (Radio Frequency IDentification) and WSN (Wireless Sensor Network) that are detected with the guide of the tremendously working sensor contraptions and are comparatively handled by involving a centralized server for deciding and the moves are executed precisely with no human impedance. In straightforward expression, we can say that IoT is the spic and span transformation of the Internet. It offers a degree wherein items can talk, plan and control themselves.

The blast of network is diffused and regularly at this point not huge to numerous people. Over network as a “horde method for discussion and exchange” is continually on, serenely on finger, records-well off and intuitive permits associations between really the entire things, following in the expanding of the IoT idea to the Internet of Everything (Fredette et al., 2012). Web of Everything grows the IoT idea by including connections to records, individuals other than (business endeavor) processes. Subsequently it consolidates other association fundamentally based standards like IoT, Internet of People (IoP), and Industrial Internet (II) (Yang, Di Martino, and Zhang, 2017). In this system we perceive the Internet of Things (IoTs) as an organization of associations between adroit issues, people, strategies, and data with ongoing realities/realities tides between them.

Aside from beatitudes of IoTs, there are a few stronghold and security worries at exceptional layers viz; Front end, Back quit and Network. This paper, the review is in a few changes in different business undertaking conditions connected with Internet of Things (IoTs) by depleting characterizing a few open difficulties. The second part thinks on how improvement in age bunch has contorted the few venture areas inside the general public to advance to relate themselves with the installed programming.

Objectives of the Study
• To understand paradigm change due to IoT in various business scenarios
• To explore how advancement in technology has transformed the countless business sectors to adapt to link them with the embedded software.
• To study the requirements and challenges of security measures in IoT.

Statement of the Problem
The highest levels of smartness of things in the IoE are brought about by connected things exhibiting an ability to adapt to unknown or unexpected circumstances, to act autonomously and to collaborate with other constituents. In turn, this implies that networks of organizations too will need to develop and apply related strategic competences, to have flexible organizational structures, relationships and processes, and to adapt quickly as new data-driven insights emerge. At higher levels of smartness, industry sectors will succumb to the ‘Winner Takes All’ pattern of power centralization unless new institution arrangements emerge to enable data sovereignty solutions. Such of these problems and challenges need to be contemplated more scientifically while making an attempt to understand and making certain that how to use IoTs at the same time not to experience too much of difficulties in terms of data safety, data seepage, and the like.
Scope of the Study

IoT capacities to allow matters to be connected wherever and each time the utilization of any help/local area. Having this reason for IoT as a main priority, it is said that a precise and clean execution of an IoT machine particularly relies upon distinguishing the right standards concerning the right disclosure, recognizable proof, design and control of interconnected gadgets and sensors. The construction of IoT must be an open design, utilizing open conventions to help many current organization applications. Similarly, it ought to also incorporate security, versatility and semantic outline middleware to advance records global reconciliation with Internet. In consideration of those thoughts and a few related investigations, when the entire thing indispensable and required are taken consideration, it’ll really be a great stage to the clients with no issues specifically so they can work pressure free.

Internet of Things (IOT) - Definitions

Throughout the long term many creators were attempting to frame the Internet of Things peculiarity with the guide of expanding the ideas of “Web” and “things”, depicting their capacities, approaches of associating and collaborating. Conversations take area or even contentions are given contrary to the utilization of the expressions “Web” and “things” because of the impedance of the human part, so the expression “Web of people” is proposed.

Ransack van Kranenburg (2011) investigates and arranges interesting meanings of the thought. One of them, given by utilizing the EU mission Casagras, makes sense of in data that IoT is “A worldwide local area foundation, connecting physical and computerized objects through the double-dealing of insights catch and dispatch abilities. This foundation incorporates current and advancing Internet and local area improvements. It will offer explicit thing distinguishing proof, sensor and association capacity as the thought for the advancement of fair-minded agreeable contributions and projects. These can be described by means of an inordinate confirmation of free data seize, event switch, network availability and intero-perability”.

Adrian McEwen gives extremely basic definition introduced by the accompanying condition:

Actual article + Controller, Sensor and Actuators + Internet = Internet of things

Wherein actuators are the results into the area created through the “matters”. This large number of definitions proposes that the circumstances that make the Internet of Things come into all circles of our ways of life are Internet.

Literature Review

Khazensiri et al. (2017) completed a survey on IoT answers for smart power control to take advantage of smart metropolitan packages. In Uphaar, IoT has been deployed in technology and very few software areas to serve the people, he added. The scope of IoT is very wide and near to destiny IoT is able to seize almost all utility sectors. He mentioned that power saving is one of the important parts of the society and IoT can help in developing a smart power control gadget which is a good way to keep every power and cash. He defined an IoT architecture with the Smart Metropolis concept identified. The authors additionally discussed the immaturity of enterprise IoT hardware and software that is hard to reach. He advised that these issues should be addressed to build a reliable, green and consumer friendly IoT system.

Alvi et al. (2018) addressed the issue of urbanization within cities. The movement of human beings from rural to city environment in the growth of the population of cities. Therefore, we want to offer smart solutions for mobility, energy, healthcare and infrastructure. Smart town is one of the important software areas for IoT developers. It explores a range of problems including visitors management, air quality control, public safety answers.
Smart Parking, Smart Lightning and Smart Garbage Collection. He said that IoT is working hard to tackle those challenging issues. The need for advanced smart city infrastructure coupled with increasing urbanization has opened doors for the marketers in the field of smart city technologies. The authors concluded that the IoT enabled era could be very important for the improvement of sustainable smart cities.

Heer et al. (2011) brought up a security issue in IP based IoT systems. He mentioned that the Internet is the backbone for the verbal exchange between gadgets that takes up territory in an IoT system. Therefore, security issues are an essential concern in IP based fully IoT systems. Furthermore, the security architecture must be designed taking into account the lifecycle and capabilities of any object within the IoT device. This also includes the involvement of 1/3rd parties and those relying on security protocols. Security architecture with scalability capability is quite acceptable in IoT to serve things ranging from small scale to large scale. As explained at a glance, IoT has given the whole community a new way of verbal exchange between many things*******, resulting in the abandonment of the traditional protocols required for this communication. are not able to provide assistance. Therefore, the new protocol must be designed with a consideration of translation at the gateway to ensure complete security. In addition, each layer responsible for releases has its own security issues and requirements. Therefore, meeting the requirements for a particular layer will directly bring the gadget into a prone kingdom and security must be ensured for all layers.

Liu et al. (2012) brought a solution to handle authentication and gain access to control. Authentication may be very necessary to verify the communicating parties to protect you from the loss of personal data. They have supplied an authentication scheme based on Elliptic Curve cryptosystem and tested it on specific security threats ie. Eavesdropping, Center Attack, Key Control and Replay Attack. He claimed that the proposed plans are capable of offering higher certification and gain entry to management in IoT based communications primarily.

Kothmayer et al. (2013) proposed a one-way authentication scheme based primarily on Datagram Transport Layer Security (DTLS) for IoT. Attackers on the Internet are constantly active in stealing secure data. The proposed technologies are capable of providing message security, integrity, authenticity and confidentiality, recall overhead and stop-to-stop latency inside IoT based communication networks primarily.

Lee et al. (2019) proposed a dynamic method for statistics-focused IoT applications with respect to cloud platforms. The need for a suitable equipment, software program configuration and infrastructure to support the massive amount of IoT programs running on cloud systems demands efficient answers. IoT developers and researchers are actively engaged in developing solutions taking into account both large systems and the heterogeneous nature of IoT items and devices.

Kim et al. (2015) addressed the difficulty of climate alternatives and proposed an IoT based primarily ecological tracking system. He noted that existing techniques are time-consuming and require various types of human intervention. Also, a normal visit is needed to get information from the sensors on the web site under investigation. Also, some data remained missing resulting in highly under-corrected evaluation. Therefore, IoT based framework is able to overcome this problem and can provide high accuracy in analysis and Prediction.

Fang et al. (2014) delivered an Incorporated Facts Tool (IIS) that integrates IoT, geo-informatics, cloud computing, Global Positioning Machines (GPS), Geographic Facts Devices (GIS) and e-technological information to make it an effective environment. Provide. tracking and management machine. They noted that the proposed IIS presents a range of advanced facts, analysis and decision-making for climate manipulation. Air pollutants are another significant difficulty internationally. There are various tools and techniques available to make good measures and control a breeze.
Major Key Issues and Challenges of IoT

The contribution of IoT based structures in all components of living souls and different advancements associated with realities switch among implanted contraptions made it muddled and gave up push to a few issues and difficulties. These issues additionally are a task for the IoT engineers inside the high level brilliant tech society. As time is creating, requesting circumstances and need for prevalent IoT device is likewise creating. In this way, IoT engineers need to consider late difficulties jumping up and should give answers for them.

Security and Protection Issues

One of the greatest significant and testing inconveniences in the IoT is the security and protection on account of a few dangers, digital attacks, risks and weaknesses (Babovic, 2016). The issues that give up push to gadget degree privateness are lacking approval and confirmation, unreliable programming, firmware, web point of interaction and unfortunate conveyance layer encryption (Hewlett Packard Enterprise Report. 2015). Security and protection issues are extremely fundamental boundaries to grow confidence in IoT Systems with appreciate to different variables (Xu LD, 2014). Security systems ought to be inserted at each layer of IoT engineering to save you security dangers and assaults (Yan Z, Zhang P, Vasilakos AV 2014). A few conventions are advanced and productively conveyed on each layer of verbal trade channel to ensure the security and privateness in IoT based absolutely frameworks (Dierks T, Allen C., 1999; Pei M, Cook N, Yoo M, Atyeo A, Tschofenig H. 2016). Secure Socket Layer (SSL) and Datagram Transport Layer Security (DTLS) are one of the cryptographic conventions which may be applied among conveyance and application layer to offer wellbeing arrangements in various IoT structures (Dierks T, Allen C., 1999). Nonetheless, some IoT applications require unique techniques to make specific the security in correspondence between IoT gadgets. Other than this, in the event that verbal trade takes region the utilization of remote innovation in the IoT framework, it will turn out to be extra vulnerable to security risks. Thusly, certain procedures should be conveyed to find malevolent activities and for self-recuperation or recuperation. Security anyway is some other significant issue which allows in clients to encounter stable and comfortness while the utilization of IoT replies. In this manner, it’s especially expected to keep up with the approval and confirmation over a consistent local area to set up the discussion among confined in occasions (Roman R, Najera P, Lopez J. 2011). Another trouble is the extraordinary security rules for special contraptions talking inside the IoT framework. In this manner, every thing ought to be fit for check the security guidelines of various devices in IoT gadget sooner than sending the information.

Interoperability / Preferred Issues

Interoperability is the feasibility of trading data between specific IoT gadgets and systems. This exchange of data no longer depends on deployed software and hardware. The interoperability problem arises because of the heterogeneous nature of the specific era and the solutions used for IoT improvement. The four interoperability tiers are technical, semantic, syntactic and organizational (Van-der-Weer H., Wills A., 2008). Various functionalities are being supplied using IoT systems to enhance the interoperability that guarantees communication between particular objects in a heterogeneous environment. Additionally, it is possible to merge specific IoT platforms based on their functionality to provide multiple answers for IoT customers (Colacovic A, Hadzialic M. 2018). Recognizing interoperability as an important problem, the researchers accepted a number of answers, which can also be referred to as Interoperability Handling Procedures (Noura M, Atikazaman M, Gedke M, 2018). These answers can be adapter/gateway based, digital network/overlay based purely, provider oriented architecture based purely etc. Although counteracting
interoperability with processes reduces some of the stress on IoT systems, certain challenges remain with interoperability that may be a scope for the study of destiny (Noura M, Atikazaman M, Gaedke M. ., 2019).

**Ethics, Regulation and Regulatory Rights**

One more trouble for IoT designers is morals, regulations, and administrative power. There are sure approaches and rules to keep up with principles, virtues and to keep individuals from abusing them in different associations. Morals and guideline are entirely practically identical time spans and the least complex distinction is that morals are necessities that individuals trust in and lawful rules are positive assents set through specialists. Be that as it may, each ethical quality and regulation is intended to protect the standard, worn out, exceptional and keep people from illicit use. With the advancement of IoT, some genuine issues have been tackled, despite the fact that it has likewise led to essential moral and jail difficulties (Tzafestad SG. 2018). Information security, security assurance, trust and security, convenience of realities are a portion of the difficulties. It has likewise been viewed that as the vast majority of the IoT clients are leaning toward government standards and guidelines in regards to somewhere safe, protection and security of realities because of absence of acknowledgment as truth in IoT gadgets. Along these lines, this issue should be considered to keep up with and work on the acknowledgment among people for the utilization of IoT gadgets and constructions.

**Scalability, Availability and Reliability**

A machine is scalable if new services, tools and gadgets are developed without needing to use out, it is possible to feature deteriorating its performance. The main problem with IoT is to support massive amounts of gadgets with specialized memory, processing, storage energy and bandwidth (Pereira C., Aguirre A., 2014). Another important issue that should be addressed is availability. Scalability and availability must each be deployed together within the layered framework of IoT. A great example of scalability is a cloud based fully IoT system that provides enough support to scale the IoT community by incorporating new gadgets, storage and processing power as needed. However, this international distributed IoT community gives rise to a new study paradigm that broadens a seamless IoT framework that meets international needs (Mosko M, Solis I, Uzun E, Wood C., 2017). Another important function is the provision of sources for appropriate goods irrespective of their location and time of need. In a distributed fashion, many smaller IoT networks are well-connected to global IoT systems to utilize their resources and offerings. Therefore, availability is a significant challenge (Wu Y, Lee J, Stankovic J, Whitehouse K, Son S, Kapitanova K., 2010). Due to the use of different statistics broadcast channels ie. Satellite TV for PC conversations, some offers and asset availability may be hampered. Therefore, there is a need for a fair and reliable fact broadcast channel for uninterrupted availability of assets and services.

**Quality of Service (QoS)**

Quality of Service (QoS) is another important component for IoT. QoS can be defined as a measure to evaluate the satisfactory, efficiency and performance of IoT devices, systems and infrastructure (Temglit N, Chibani A, Djouani K, Nacer, 2018). Important and essential QoS metrics for IoT programs are reliability, price, energy intake, security, availability and service time (Huo L, **** Z., 2016). A smart IoT environment needs to meet the requirements of QoS standards. Also, to ensure the reliability of any IoT provider and device, its QoS metrics must first be described. In addition, users will be able to specify their needs and requirements as well. Several approaches can be deployed for QoS assessment, although as noted using White et al. (2017)
There is a compromise between exceptional elements and processes. Therefore, precisely the right models must be deployed to win this alternate-off. There are some true fine models available in the literature including ISO/IEC25010 (Technical Report; 2010) and OASIS-WSQM (2012) that can be used to evaluate strategies used for QoS assessment. These models best present a wide range of factors which is sufficient for QoS evaluation for IoT offerings.

Discussions

According to Gartner’s assessment and forecasts, there could be 20 billion related gadgets on Earth by the end of 2020. BI intelligence is estimated to reach over 24 billion and nearly $6 trillion could be spent on IoT answers over the next 5 years (Business Insider 2017). It will alter the way IoT related businesses operate. They should invest money in Internet of Factor hardware and optimize workflows, rework new commercial enterprise models and regulate traditional employer roles, ensure cyber security and customer privacy (Kaleel Ahmed A, CB Senthil Kumar 2017).

From a micro perspective, finishing matters with smartness can significantly change not only the career provisioning for the client, but also the painting environment of the frontline career employee. From a customer perspective, finishing matters with smartness allows for higher, more customized and personalized products and services that provide further convenience (Rust & Huang, 2014). They additionally allow delegating duties to the patron, hence saving effort and time. For example, when modern connected motors are installed, without the intervention of a patron, for the desired software replacement, they save the consumer the hassle of negotiating with a car maintenance company (Porter & Heppelman, 2014). These blessings of smartness power increase consumer attractiveness of smart gadgets, which is likely to improve with increasing levels of smartness. However, at very high levels of smartness, issues with security, privacy, and trust become more relevant (Papadopoulou, Kolomvatsos, Panagidi, & Hadjiphthymieds, 2017).

According to our classification, as an example, things with a low level of smartness are best reactive at the same time because people with a high level of smartness are self-sufficient and able to cooperate that allows you to achieve their goals. gives. While business enterprise models can also create conflict on a micro level, the change of institutions, and there with the gadgets of rules governing interactions, is often provoked through people. Human competencies have the ability to mitigate hazards and the effects of smartness to ensure that fee introductions take place, and they are also able to do the institutional painting necessary to develop new readiness (Lawrence & Sudabi, 2006) are capable.

As a third point of view in this discussion, we take into account key studies seeking conditions at the macro stage, as IoE and smart stuff change the value ecosystem within enterprise sectors in addition to enterprise sectors. The classification proposed in this paper demonstrates that as connected things gather higher levels of smartness, some materials within and between industry sectors using shared data and developing a fluid and bendy commercial enterprise fashion into a single IoE become part of the community. This has resulted in industry convergence (Ill, Preschitschek, Laker, & Broering, 2019), new networked enterprise fashions (Edner, 2017; Bankwall et al., 2017; Oskum et al., 2018), and new carrier ecosystems (Hacklin, 2015). Batistini) results. , and von Krogh, 2013). Established enterprise barriers become blurred and fragmented and industries cease to exist in isolated regions. New venture outsiders invest in the market and define new paradigms, often within the size of IoE-enabled offerings or as opposed to physical business. This does not mean that character organizations must incorporate the emergence of smart cases and optimize their enterprise models, their operations and their cost ecosystem, but also that entire regions or economies must do so simultaneously. So a key function appears to be guiding organizational decision-making about which networks to participate in, and how to find the appropriate partners.
for value co-creation. Such a move into uncharted territory brings substantial problems aligning institutional preparedness among hitherto unconnected areas (Besharov & Smith, 2014). Despite these impending changes, many companies struggle to recognize the dynamics of IoE-enabled industry convergence and its associated demand conditions and prospects (Kim, Hyokseong, Kim, Lee & Suh, 2015). Disruption resulting from enterprise convergence creates a complex, fluid and uncertain environment where sustainable strategic choices are difficult to make (Hacklin et al., 2013).

**Recommendations**

As businesses are actually incorporating a variety of innovations into their workplaces and more workspaces are becoming equipped with IoT apps, an initiative has begun to leverage the momentum towards a smarter administrative center. Many connected devices are used by workplaces to tune, manipulate and control specific operations in an agency. Using IoT technology capable of connecting gadgets will allow remote painting inside the work space to increase worker productivity. To facilitate collaboration, employees may no longer be required to live with every other worker within the same workplace. If a workplace takes advantage of a shared network, employees can do their jobs elsewhere using portable devices and cloud-hosted programs. Keep in mind that first-class technology to improve people’s productivity is IoT-based entirely in place of job initiatives. When more corporations and the general public use technology and smart devices in their normal lives, security becomes a higher issue. Using IoT generation to ensure that a green place at work security plan will help prepare for viable cybersecurity threats that can steal facts.

The method will be simplified as it moves forward as IoT is implemented in the office space. The stock control department of an agency will enjoy the IoT stuff related to asset tracking. The vast amount of information derived from IoT devices makes IoT profitable for corporations. The collected records can be used for extracurricular use for additional daily tasks. IoT especially can enhance B2C (business-customer) engagement. It provides an exciting new method for companies to communicate with their customers and can digitize in addition to automating tons of interactions. When this period becomes more affordable and without the problems at hand, any employer can take advantage of it and be able to successfully improve their performance.

**Conclusion**

Without a doubt, the quick enhancements of new advancements influence all region of the overall way of life and the provided examination and audits show that these improvements will be supported and created in ongoing years. Regardless of whether we want it, we are essential for this innovative transformation and the main thing is to figure out how to utilize it well and shrewdly. Consequently the endeavors of all gamers in the realm of Internet of Things - apparatus transporters, administrators, stage suppliers, framework integrators, utility sellers, states and customers to join to establish a steady and secure elimate for verbal trade and business of private Will occur. Truth. The combination of the Internet of Things ought to stick to a certain inventive and prescience and thought, distinguish the conceivable outcomes of purpose of the time, appeal to business undertaking foundations and specialists, and embrace a way of life to utilize the Internet of Things should assemble.

In this paper, the change in outlook occurring in different venture situations, how the development of age has changed numerous areas, the security guidelines of IoT are explicitly assessed and the manner in which many organizations are inserted inside the current changed examples. Associating yourself to the product, The prerequisites and request conditions for safety efforts in IoT have been examined and procured under different headings. A wide range of safety
dangers that could be basic to the turn of events and execution of IoT in explicit regions were noted and sorted with acknowledgment of the layers of the IoT design: trust layer, local area layer, support layer, and readiness. Layer. At long last, ongoing answers for those dangers were provided and with enthusiasm for security concerns research bearings have been joined with cryptographic components and firewalls.

References
1. Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. Journal of Management, 43(1), 39–58. https://doi.org/10.1177/0149206316678451.
2. Alavi AH, Jiao P, Buttlar WG, Lajnef N. Internet of things-enabled smart cities: state-of-the-art and future trends. Measurement. 2018;129:589–606.
3. Babovic ZB, Protic V, Milutinovic V. Web performance evaluation for internet of things applications. IEEE Access. 2016;4:6974–92.
4. Bankvall, L., Dubois, A., & Lind, F. (2017). Conceptualizing business models in industrial networks. Industrial Marketing Management, 60(1), 196–203. https://doi.org/10.1016/j.indmarman.2016.04.006.
5. Besharov, M. L., & Smith, W. K. (2014). Multiple institutional logics in organizations: Explaining their varied nature and implications. Academy of Management Review, 39(3), 364–381. https://doi.org/10.5465/amr.2011.0431.
6. Colacovic A, Hadzialic M. Internet of things (IoT): a review of enabling technologies, challenges and open research issues. Comput Netw. 2018;144:17–39.
7. Dierks T, Allen C. The TLS protocol version 1.0, IETF RFC, 2246; 1999. https://www.iETF.org/rfc/rfc2246.txt.
8. Fang S, et al. An integrated system for regional environmental monitoring and management based on internet of things. IEEE Trans Ind Inf. 2014;10(2):1596–605.
9. Fredette, J., Marom, R., Steinert, K., & Witters, L. (2012). The promise and peril of hyperconnectivity for organizations and societies. The Global Information Technology Report. World Economic Forum. https://www3.weforum.org/docs/GITR/2012/ GITR_Chapter1.10_2012.pdf
10. Hacklin, Battistini, & Von Krogh, (2013), Strategic Choices in converging industries, Sloan Management Review, Vol 55, No.1, PP 65-73.
11. Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K. Security challenges in the IP based internet of things. Wirel Pers Commun. 2011;61(3):527–42.
12. Here’s how the Internet of Things will explode by 2020, http://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2?IR=T, 2016.
13. Huo L, Wang Z. (2016) Service composition instantiation based on cross-modified artificial Bee Colony algorithm. Chin Commun. 2016;13(10):233–44.
14. Internet of Things research study: Hewlett Packard Enterprise Report. 2015. http://www8.hp.com/us/en/hp-news/press-release.html?id=19090 50#.WPoNH 6KxWU k.
15. ISO/IEC 25010—Systems and software engineering—systems and software quality requirements and evaluation (SQuaRE)—system and software quality models, Technical Report; 2010.
16. Kaleel Ahmed A, C.B. Senthil Kumar, Correlating Internet of Things, International Journal of Management (IJM), Volume 8, Issue 2, pp.68–76, 2017
17. Khajenasiri I, Estebsari A, Verhelst M, Gielen G. A review on internet of things for intelligent energy control in buildings for smart city applications. Energy Procedia. 2017;111:770–9.
18. Kim NS, Lee K, Ryu JH. Study on IoT based wild vegetation community ecological monitoring system. In: Proc. 2015 7th international conference on ubiquitous and future networks, Sapporo, Japan, 7–10 July 2015. IEEE.
19. Kim, N., Hyeokseong, L., Kim, W., Lee, H., & Suh, J. H. (2015). Dynamic patterns of industry convergence: Evidence from a large amount of unstructured data. Research Policy, 44(9), 1734–1748. https://doi.org/10.2139/ssrn.2519054.
20. Kothmayr T, Schmitt C, Hu W, Brunig M, Carle G. DTLS based security and two-way authentication for the internet of things. Ad Hoc Netw. 2013;11:2710–23.
21. Kranenburg, R., The Internet of Things, draft paper prepared for the 1st Berlin Symposium on Internet and Society, 2011
22. Lawrence & Suddaby,R. (2006), Institutions and institutional work. In S.R.Clegg, C.Hardy, T.B.Lawrence & W.R.Nord(Eds.)Sage Handbook of organization studies (PP-215-254), London: Sage.
23. Li Y, et al. IoT-CANE: a unified knowledge management system for data centric internet of things application systems, Journal of Parallel Distib Comput. 2019;131:161–72.
24. Liu J, Xiao Y, Philip-Chen CL. Authentication and access control in the internet of things. In: 32nd international conference on distributed computing systems workshops, Macau, China. IEEE xplore; 2012. https://doi.org/10.1109/icdcs w.2012.23.
25. Mosko M, Solis I, Uzun E, Wood C. CCNx 1.0 protocol architecture. A Xerox company, computing science laboratory PARC; 2017.
26. Noura M, Atiquazzaman M, Gaedke M. Interoperability in internet of things: taxonomies and open challenges. Mob Netw Appl. 2019;24(3):796–809.
27. Noura M, Atiquazzaman M, Gaedke M. Interoperability in internet of things infrastructure: classification, challenges and future work. In: Third international conference, IoTaaS 2017, Taichung, Taiwan. 20–22 September 2017.
28. Oasis. Web services quality factors version 1.0. 2012. http://docs.oasis-open.org/wsqm/wsqf/v1.0/WS-Quali ty-Facto rs.pdf.
29. Oskam, I., Bossink, B., & de Man, A. P. (2018). The interaction between network ties and business modeling: Case studies of sustainability-oriented innovations. Journal of Cleaner Production, 177, 555–566. https://doi.org/10.1016/j.jclepro.2017.12.202.
30. Papadopoulou, Kolomvatsos, Panagidi, & Hadjiefthymiades, (2017), “Investigating the potential of Internet of Things”, Proceedings of the Mediterranean Conference on Information Systems, PP 1-14.
31. Pei M, Cook N, Yoo M, Atyeo A, Tschofenig H. The open trust protocol (OTrP). IETF 2016. https://tools.ietf.org/html/draft -pei-opent rustp rotoc ol-00.
32. Pereira C, Aguiar A. Towards efficient mobile M2M communications: survey and open challenges. Sensors.2014;14(10):19582–608.
33. Pereira C, Aguiar A. Towards efficient mobile M2M communications: survey and open challenges. Sensors. 2014;14(10):19582–608.
34. Porter.M. & Heppelman.J.E. (2014) “How smart connected products are transforming competition”, Harvard Business Review, Vol 94,(1-2), PP 1-23.
35. Roman R, Najera P, Lopez J. Securing the internet of things. Computer. 2011;44(9):51–8.
36. Rust, R. T., & Huang, M. H. (2014). The service revolution and the transformation of marketing science. Marketing Science, 33(2), 206–221. https://doi.org/10.1287/mksc.2013.0836.
37. Sick, N., Preschitschek, N., Leker, J., & Bröring, S. (2019). A new framework to assess industry convergence in high technology environments. Technovation, 84–85, 48–58. https://doi.org/10.1016/j.technovation.2018.08.001.
38. Temglit N, Chibani A, Djouani K, Nacer MA. A distributed agent-based approach for optimal QoS selection in web of object choreography. IEEE Syst J. 2018;12(2):1655–66.

39. Tzafestad SG (2018) Ethics and law in the internet of things world. Smart Cities. 2018;1(1):98–120.

40. Van-der-Veer H, Wiles A. Achieving technical, interoperability-the ETSI approach, ETSI White Paper No. 3. 2008. http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Ed%20final.pdf.

41. White G, Nallur V, Clarke S. Quality of service approaches in IoT: a systematic mapping. J Syst Softw. 2017; 132:186–203.

42. Wu Y, Li J, Stankovic J, Whitehouse K, Son S, Kapitanova K. Run time assurance of application-level requirements in wireless sensor networks. In: Proc. 9th ACM/IEEE international conference on information processing in sensor networks, Stockholm, Sweden, 21–16 April 2010. p. 197–208.

43. Xu LD, He W, Li S. Internet of things in industries: a survey. IEEE Trans Ind Inf. 2014;10(4):2233–43.

44. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for internet of things. J Netw Comput Appl.2014; 42:120–34.

45. Yang, L. T., Di Martino, B., & Zhang, Q. (2017). Internet of everything (editorial). Mobile Information Systems, 2017, 1–3.