Integrating internet of things: A review on the effects on the future of the global community, challenges faced and security, privacy and perspective measures

AfreenBhumgara
NowrosjeeWadia College
Pune, India
afreenbhumgara97@gmail.com

Abstract*: The use of internet has become one of the modern ways of sharing information, data and documents. The need to deign it in such away that it becomes quicker and reliable therefore becomes the major challenge. Internet of things becomes ideal at this point in time since it provides a connectivity that solves the above problem.IoT technology is affecting the global community and billions and billions of connected devices are secured as the Internet of Everything continues to skyrocket.We have thousands of choices for hardware, operating systems, and chipsets that continue to push the Internet of Things forward. Hardware is becoming more accessible, inexpensive, and easier to use.According to SoftLayer's Joshua Krammes, building Community around you IoT Brand not only creates awareness but also increases market penetration of the same. Home automation will see an explosion in products over the next few years. The number of connected smart devices is rapidly increasing, with 50 billion devices possible by 2020. According to Peter Friess (2014).50% of the world's population currently lives in cities and the need to make our future cities more intelligent and connected has never been greater than before.How can these cities be designed to fit the ever changing connectivity need?As networks advance at a high rate, there is the changeover of networks from closed to open enterprise ones. Besides, the utilization of smart devices especially in surging is becoming more popular. Consequently, fears are rising when it comes to data security. On the same note, the increased reliance on the Internet of things technology makes it difficult to not only monitor, but also protect both public and personal information. In most cases, IoT requires organizations to gather and maintain data efficiently. It also requires that organizations monitor the authorization of data usage in a controlled mannerism.*

Keywords*:*

I. INTRODUCTION

This section introduces us to the research study. It consists of background of the research, significance of the research, research rationale, scope, questions, hypotheses, aim, and objectives.

A. Background of the Research

Nowadays governments start to consider ICT as the main driver, which will lead to fundamental changes in many aspects of modern society: environment, healthcare, security and many other areas. Furthermore, government agencies search for opportunities to standardize these processes. Internet of Things can not only improve the efficiency of various industries but also to present a completely new business models that have never before been used in traditional industries. Thus, gradually disappears clear separation between industries, all areas of modern life will be combined into a single network. As a result, the Internet of Things becomes a factor, which entails a number of significant positive changes in society, business and government.On another side, Internet of Things is built on the basis of the Internet. Iot here is a risk of security problems. Since IoT contains three layers: perception layer, transportation layer, and application layer, in the paper it will be analyzed the security problems of each layer separately and try to find solutions. The internet of things has had diverse contributions to enhancing connectivity of both individuals and organizations. Its benefits are evident in diverse sectors and continue to change the manner in which entities operate. Its unmatched contribution to the progress of organizations and economies, however, is subject to diverse challenges and concerns. Key among such concerns is the susceptibility of the internet of things to cyber insecurity. Analysts have questioned the extent to which the internet of things promises security to its users. The concerns of contemporary threats posed by cyber insecurity are real and have potential implications on the

functionality of the internet of things. Such threats prompt studies to evaluate the extent to which the internet of things remains resilient and resolute to withstand the challenges. Cyber resilience is the fundamental concept as outlined in ISO 27001 in an attempt to ensure entities dependent on the internet of things are sure of their continuity and protection from cyber threats. This research probes the question as to the extent to which the internet of things remains cyber resilient. It underscores the core aspects of cyber resilience and investigates the key factors that would ensure its conformity in regards to the internet of things. Today, in the era of globalization, the role of Internet has become one of the most important parts in our life. It can be defined as a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide, it is also considered as a huge electronic library of humanity which contains a lot of information and knowledge. Therefore, it is probably to say that people cannot live without Internet today, however, the Internet has both its advantages and disadvantages. In the positive side, there is one thing that we can see easily is that Internet can be used to communicate people from every part in over the world within a few clicks.

B. Significance of the Research

Information technology has brought a new wave to our education system. This availability has changed the education system in such a way that people do not have to be physically present in school to learn. The availability of number of online classes and schools has also increased lately and there is an availability of various subjects. The online education programs are popular today and currently serve various sections of the population. As it is fairly new, it still undergoes change in policies and course structures. Importantly, the roles of teachers have also changed as teaching in an actual class is no longer mandatory and online classes are significantly different in communication, interaction and tools. There was a common misconception that online courses actually require more commitment and interaction among classmates and the facilitator. It was found that in the early days of distance education there was hardly any change in the context of traditional teaching methods. However, in the new model of online classes more emphasis is given to activities like group –projects, assignments and collaborative discussions among students and faculties. Thus, as a result, it has been found that there is an increased involvement and excelled interaction between students and faculties than before.

C. Research Rationale

Internet of things is the interconnection of physical devices with electronics; software's, sensors and network connectivity to enable these devices collect and exchange data. This allows objects to be sensed and be controlled remotely. It helps to create opportunities for more direct integration of computer based system resulting to efficiency and accuracy. When loT is augmented with a sensor, the technology becomes an instance of cyber-physical system that encompasses technology. Each thing is uniquely identified through an embedded computer system but also incorporates existing internet infrastructure.

D. Scope of the Research

E. Research Questions

The research will address the following questions:

- Do usable and useful systems improve usability to enhance user experience?
- Are interactive frameworks in the portable, omnipresent, and virtual situations at a phase of advancement where creators and engineers are quick to discover more about the outline, use, and ease of use of these frameworks?
- Do sensing and scale hold responsible for causing ubiquitous computing systems to resist iteration prototype creations?

F. Research Hypothesis

- **H1** Useful systems enhance user experience and consumer's satisfaction.
- **H2** Interactive frameworks create ubiquitous systems built on reliability.

G. Research Aim and Objectives

The aim of the research is to analyze ubiquitous computing systems in order to suggest improvisations and outline the pros of improved systems.

Objectives of the research will be:

- To assess the tools and techniques for designing, implementing, and evaluating ubiquitous computing systems used by developers
- To formulate practical solutions that addresses the functionality of these systems.

II. RESEARCH METHODOLOGY

This section emphasizes the methodology and techniques for this research and the pattern considered most appropriate for this study. It is made up of the research purpose, study design, ethical considerations, and challenges encountered in the course of the research.

A. Research Purpose

This is a theoretical research with the sole aim of providing emphasized descriptions of various phenomenon and conditions persistent which are connected to situations, individuals, or occurring events. The aim of the research is to generalize the outcomes of theories which develop over the course of the study. Along with that, a descriptive and theoretical research is always carried out on the basis of sufficient knowledge of the researcher with hypotheses based on the questions and that there is not intent to investigate the clauses between situations and occurring events. Empirical study gained from literature review and secondary data are involved in most aspects of the research. Analysis and derivations are used as evidence or proof.

B. Study Design

The study design is a mixture of empirical and theoretical study design. Theoretical aspect accrues data from mathematical modelling and empirical aspect is in the use of available literature evidence in substantiating the assertions. The advantages of this design is because it is cheap, less time consuming, and it enables the comparison of data to come up with valid and reliable findings.

C. Ethical Considerations

The study adhered to the principal ethics requirements. Permission to proceed with this research was obtained from relevant authorities. The studies selected for the literature review met the ethical requirements and they were published in the public domain. The authors of the literature reviewed for secondary data were accredited in both the in-text citation and reference page for conformity to policy against plagiarism.

D. Challenges Encountered

Several challenges were encountered in this research. Given that it is a mixed study, the outcome of the literature review may not correlate with the theoretical modelling findings because as one is theoretical the other one is empirical evidence. It was cumbersome to get sufficient peer reviewed papers relevant to this topic because the field is least researched due to its rapid advancement. The time was limited and financial constraints experienced necessitated cheap and less time consuming study designs to be selected for the research.

III. RESULTS OF THE RESEARCH

This section presents the findings of the research. It provides results of the research on the available body of knowledge in regards to the topic of the study, which constitutes a review of relevant literature. It also provides the evidence obtained in the mathematical modelling section to come up with valid and reliable assertions. The results from empirical evidence and mathematical modeling are analyzed to provide credible conclusions.

A. Findings from Empirical Evidence Reviewed

The innovations and development in the globalized business world have allowed to businesses to share or transact information rapidly and easily. On the other hand, organizations have also utilized these developments for conducting their business activities through digital mediums and started using online platforms for commerce. E-commerce has created an opportunity for the business to use a more convenient platform to reach mass market and the researches have shown that almost 80% of the business activities especially transactions are being conducted online (Cleveland, 2008). Therefore, the need of security and transparency in this field is very high and of immense importance. These transactions are conducted online which is why making the online mediums secure and safe should be the top most priority of organizations. This is where the concept of cyber security has emerged and came into existence. The need was there as the businesses were seeking convenience but it also poses a threat. However, most of the people working in the IT sector or dealing in cyber security insist that cyber security only deals in making the IT systems within an organization secure (Ericsson, 2010).The advancement in the internet technology such as accessing the internet via mobile phones has increased the number of people using these services. One of the concerns that comes with the increased access is an authorized access to personal information available on the internet. This has given birth to the term cyber security that is aimed at protecting users of the internet as well as the information available on the internet on peoples' accounts. The increasing concerns on cyber security have led to efforts by different scholars to establish the most effective ways to ensure security in the access of the internet. Further, the increasing access to the internet has complicated the realization of effective means that can be used to meet the needs of all users. However, some of the most effective security measures that have been identified include use of passwords, setting verification codes, linking accounts to mobile phone numbers, among others. However, it remains important to conduct more studies that are aimed at edifying the masses on the available measures so that effective choices can be made. This study will present a review of the existing security measures, highlight the most used measures, and recommend necessary improvements. The new field of "ubiquitous computing" [1] or "ambient intelligence" [2] has brought computing capabilities to the physical context and has expanded the intelligence of objects surrounding us. Actually we have gone from smart place to smart objects in which objects can interact with each other and with people. In 2005 The International Telecommunication Union UIT published a report named "ITU Internet Reports 2005: The Internet of Things" [3]. This publication is part of the series of "ITU Internet Reports". It looks at the next step in which new ubiquitous technologies (such as Radio frequency Identification and sensors) promise a world of networked and interconnected devices that provide relevant content to users. This publication covered a review of enabling technologies, business opportunities, public policy challenges, and implications for the developing world.We are witnessing the dawn of a new era of Internet of Things (IoT; also known as Internet of Objects). Generally speaking, IoT refers to the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence. IoT will increase the ubiquity of the Internet by integrating every object for interaction via embedded systems, which leads to a highly distributed network of devices communicating with human beings as well as other devices. Thanks to rapid advances in underlying technologies, IoT is opening tremendous opportunities for a large number of novel applications that promise to improve the quality of our lives. In recent years, IoT has gained much attention from researchers and practitioners from around the world. This special issue is focused on the latest results in the area of IoT.

B. Improvement measures, Security Protocols and Perspective Gains

References

1. Weiser, M. The Computer for the Twenty-First Century. Scientific American 265(3), pp. 94-104, September 1991.
2. Ahola J (2001) Ambient Intelligence, ERCIM News, No 47, October 2001. Available in: http://www.ercim.org/publication/Ercim_News/enw47/intro. html

3. Dawson, M., Eltayeb, M., & Omar, M. (Eds.). (2016). Security Solutions for Hyperconnectivity and the Internet of Things. IGI Global.
4. Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23-30.
5. Cleveland, F. M. (2008). Cyber security issues for advanced metering infrastructure (ami). In Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE (pp. 1-5). IEEE.
6. Ericsson, G. N. (2010). Cyber security and power system communication—essential parts of a smart grid infrastructure. Power Delivery, IEEE Transactions on, 25(3), 1501-1507.
7. Jones, L. K. (2015). The insecurity of things: How to manage the internet of things (Doctoral dissertation, UTICA COLLEGE).